Mestrado em Engenharia Informática

Estágio 2014/2015

Relatório Final

Avaliação do ambiente de controlo dos SI/TI e do risco de segurança de informação

Mariana Sofia Fernandes Moutinho

mariana@student.dei.uc.pt

Orientadores:

Prof. Doutor Alexandre Miguel Pinto

Miguel Barão da Cunha

Data: 02 de Setembro de 2015

FCTUC DEPARTAMENTO
DE ENGENHARIA INFORMÁTICA
FACULDADE DE CIÊNCIAS E TECNOLOGIA
UNIVERSIDADE DE COIMBRA

Avaliação do ambiente de controlo dos SI/TI e do risco de segurança de informação

Tese submetida para obtenção do Grau de Mestre em Engenharia Informática

2014/2015

Autor:
Mariana Sofia Fernandes Moutinho

Orientadores:
Prof. Doutor Alexandre Miguel Pinto
Miguel Barão da Cunha

Júri arguente:
Prof. Doutor Álvaro Rocha

Júri vogal:
Prof. Doutor João P. Vilela

02 de Setembro de 2015

Resumo

Os sistemas de informação de uma empresa podem apresentar riscos ao nível da segurança de informação, e o impacto que estes podem ter, refletem-se tanto na saúde financeira como na continuidade de negócio.

Uma empresa angolana operadora de telecomunicações com problemas na correta captação da receita, contactou a Deloitte para identificar e corrigi-los. Para iniciar o trabalho foi necessário realizar um levantamento dos processos de negócio da operadora com impacto na receita, para descobrir todos os fluxos da mesma. Simultaneamente, realizaram-se testes de integração da receita nos SI/TI, para os processos de consumos e carregamentos. Estando os processos de negócio levantados, identificaram-se os riscos associados à receita da operadora, que foram apresentados à administração da mesma. Esta, com base na conclusão dos testes de integração, decidiu que seria necessário realizar uma auditoria aos SI/TI, que realizam o processo de faturação. Esta decisão, direcionou o trabalho apenas para os riscos de segurança de informação, onde foram identificados os respetivos objetivos e atividades de controlo. De forma a avaliar a implementação das atividades de controlo, desenharam-se testes que permitiram identificar vulnerabilidades aos controlos realizados aos SI/TI. Com esta auditoria elaborou-se uma listagem de oportunidades de melhoria que, sendo implementadas, irão mitigar os riscos associados aos SI/TI.

Palavras-chave: atividades, controlos, mitigação, risco, recomendações.

Abstract

The information systems of an enterprise may present risks in terms of information security, and the impact they may have, are reflected both in the financial health and in business continuity.

An Angolan telecommunications operator company with problems in the correct capture of revenue, contacted Deloitte to identify and correct them. To start the work it was necessary to conduct a survey of the operator's business processes with an impact on revenue flows to discover all of it. Simultaneously, there were revenue integration testing's in IS / IT to the processes of consumption and loads. Being the business processes raised the associated operator revenues risks were identified, which were presented to the respective administration. They, based on the completion of integration testing, decided it would be necessary to conduct an audit of IS / IT, which perform the billing process. This decision, directed the work only for the information security risks, where the respective objectives and control activities have been identified. In order to assess the implementation of control activities, tests were designed to have identified vulnerabilities in the controls carried out to IS / IT. With this audit it was drawn up an improvement opportunities list, that if being implemented, will mitigate the risks associated with IS / IT.

Key words: activities, controls, mitigation, risk, recommendations.

Agradecimentos

Ao João Carlos Frade, pela prontidão com que aceitou a proposta de estágio e por todo o acolhimento no departamento de Auditoria ERS TMT, Deloitte.

Ao Miguel Barão da Cunha, pelos ensinamentos, rigor, acompanhamento e toda a orientação concedida ao longo deste ano.

Ao professor Alexandre Miguel Pinto, pelas críticas, confiança, conselhos e ajuda muitas vezes fora de horas.

À equipa de ERS, pela disponibilidade constante, pela ajuda, conselhos e críticas. Acima de tudo, pela boa disposição e amabilidade com que me receberam e acolheram.

À Carolina Patrocínio, João Nunes e João Pires, pelos intermináveis debates de ideias e dúvidas, pela ajuda, pela presença, pelas palavras e amizade.

Ao João d'Assunção, por toda a ajuda, carinho, presença, amizade e amor.

Aos meus pais, irmã e Ricardo. Pelo suporte, amor, dedicação e educação.

Aos meus amigos, Gil Hilário, Cátia Costa, Joana Belém, João Farias, João Rafael, José Ribeiro, Miguel Bernardes, Pedro Cristina, Rafael Lourenço, Sara Monteiro e Telmo Neves simplesmente pela amizade e companheirismo ao longo do curso.

A todos, um sincero e sentido "Obrigada".

Índice

Lista de imagens

Lista de tabelas

Glossário

Ação corretiva - atividade para eliminar a causa de uma não conformidade detetada ou situação indesejável;

Ameaça - motivo potencial de um incidente indesejado, o que pode resultar em prejuízos para um sistema ou entidade;

Análise de risco - uso sistemático de informações para identificar fontes e calcular a probabilidade de ocorrência de um risco;

Auditoria - 1) conjunto de procedimentos usado para examinar e avaliar os registos, a fim de determinar o nível de fiabilidade, exatidão e adequação das funções da organização; 2) Intervenção de análise e diagnóstico da organização e da sua gestão para assegurar a validade, coerência e racionalização de um dado número de processos. (Carneiro, 2001);

CDR (*Call Detail Records*) - ficheiros que contêm o registo das comunicações de voz, dados e SMS;

Confidencialidade - propriedade que garante que a informação não está disponível ou revelada a indivíduos não autorizados, entidades ou processos;

Controlo de acesso - conjunto de meios para assegurar que a entrada a ativos está autorizada e é restrita com base na função do trabalho e nos requisitos de segurança;

Disponibilidade - propriedade de ser acessível e utilizável por uma entidade autorizada;

Entendimento - realizar a compreensão de determinado tema;

Evidência - qualquer tipo de dados que pode comprovar se uma afirmação é verdadeira ou falsa;

Gestão de risco - atividades coordenadas para dirigir e controlar uma organização em relação a um determinado risco;

Integridade - propriedade de proteger a exatidão de ativos;

Jobs/ batch – processo que corre em *background* em períodos pré-programados, normalmente sem existir interação humana. [1];

Mapeamento - correlação ou correspondência que se estabelece entre elementos de mais de um conjunto (Carneiro, 2001);

Matriz de segregação de funções - matriz descrevendo uma separação entre funções de autorização (perfis), de forma a que nenhum utilizador contenha poderes e atribuições desadequados às suas funções;

Nagios - aplicação que monitoriza a rede. Esta ferramenta pode monitorar tanto *hosts* quanto os serviços, gerando alertas, quando ocorrerem problemas e também quando os problemas são resolvidos (community, 2015);

Política de informação - intenção e direção geral como formalmente expressas pela gestão;

Reconciliação - comparação entre os dados que entram num determinado sistema e os dados que saem desse mesmo sistema (Carneiro, 2001);

Rede GSM (rede *Global System for Mobile Communications*) - tecnologia de redes móveis;

Risco de Segurança da Informação - potencial que uma ameaça explore uma vulnerabilidade de um ativo ou grupo de ativos e, assim, causar danos à organização;

Segregação de funções - repartição do trabalho e das responsabilidades para assegurar um controlo recíproco (Carneiro, 2001);

Segurança da Informação - preservação da confidencialidade, integridade e disponibilidade das informações;

Sistema de Gestão - âmbito das políticas, procedimentos, diretrizes e recursos associados para alcançar os objetivos de uma organização;

Sistema de Gestão de Segurança de Informação - parte do sistema de gestão global, com base numa abordagem de risco de negócio, para estabelecer, implementar, operar, monitorizar, rever, manter e melhorar a segurança da informação;

Vulnerabilidade - fraqueza de um ativo ou controlo, que pode ser explorado por uma ameaça; e

Workpapers - documentos legais necessários numa auditoria financeira de uma empresa. Esses documentos são propriedade da empresa de contabilidade responsável pela auditoria e são formalmente referidos como "Documentação de Auditoria" ou também "Ficheiro de Auditoria".

Acrónimos

AC - Atividades de controlo
AD - *Active Directory*
AIN - Análise de impacto de negócio
AS/2 – *AuditSystem/2*
BCM - *Business Continuity Management*
BCP - *Business Continuity planning*
BD - Bases de dados
BPMN - *Business Process Modeling Notation*
CDR - *Call Detail Records*
CGI - Controlo Geral Informático
CObIT - *Control Objectives for Information and related Technology*
CPD - Centro de Processamento de Dados
DRP - *Disaster recovery plan*
EDA - *Exploratory data analysis*
ERS - *Enterprise Risk Services*
GCN - Gestão de continuidade de negócio
IEC - *International Electrotechnical Commission*
IM - *Incident Management*
ISACA - *Information System Audit and Control Association*
ISO - *International Organization for Standardization*
ITIL - *Information Technology Infrastructure Library*
NPP - Faturas de consumos relativamente aos clientes
OC - Objetivos de controlo
PDCA - *Plan – Do – Check – Act*
PMO - *Project Management Office*
PNO - Parceiro de negócio da operadora
POS - *Point of sale*
RACK - *Risk and Control Knowledgebase*
RAIT - Riscos associados aos IT
RH - Recursos humanos
RIM - Deloitte's Risk Intelligence Map
SAP - Systems, Applications & Products in Data Processing
SGSI - Sistema de Gestão de Segurança de Informação
SI - Sistemas de informação
SI/ TI - Sistemas de Informação/ Tecnologias de informação
SLA - *Service Level Agreement*
SO - Sistema Operativo

TI - Tecnologias de informação
TMT - *Technology, Media & Telecommunication*
TQM - *Total Quality Management*
UPS - *Uninterruptible power supply*
VPN - *Virtual Private Network*

1. Introdução

Este documento refere-se ao estágio que decorreu na empresa Deloitte, integrado no departamento de *Enterprise Risk Services* (ERS) na área de *Technology, Media &Telecommunication* (TMT) com a duração de um ano letivo, no âmbito do processo para a obtenção do grau de Mestre em Engenharia Informática pela Faculdade de Ciências e Tecnologias da Universidade de Coimbra.

Este relatório de estágio documenta todo o trabalho realizado, desde a integração numa equipa, conhecimento do cliente e respetivo negócio, bem como a aprendizagem de várias metodologias, tecnologias e ferramentas necessárias para a realização do trabalho, fazendo desta forma a ponte entre a componente letiva do Mestrado com a aplicação prática em contexto laboral.

Neste primeiro capítulo pretende-se que o leitor conheça a entidade acolhedora e se familiarize com o âmbito do projeto e os objetivos gerais que o desencadearam.

1.1. Enquadramento

A Deloitte é uma empresa que prima em primeiro lugar pela qualidade dos seus funcionários, por isso quando um funcionário é admitido na empresa passa por um período, normalmente de um mês, de formação interna. Neste caso, a formação incidiu sobre boas práticas internas da empresa, metodologias internas e ferramentas de auditoria.

Após o período de formação deu-se início ao trabalho de auditoria. Este foi realizado para uma empresa de referência de telecomunicações angolana, que identificou a necessidade de avaliação e controlo de riscos de segurança de informação dentro da sua organização.

A equipa da Deloitte foi inserida na equipa de Receita e Faturação do cliente; em conjunto estas equipas realizaram procedimentos, tendo por base os normativos de referência (e.g. CobIT, ISO/ IEC 27001 e 22301) e ferramentas computacionais, para detetar as falhas de captação e controlar a receita. A equipa de Receita e Faturação tem como função realizar a reconciliação de toda a receita que entra na operadora.

Neste relatório o cliente de telecomunicações foi designado como "operadora".

O trabalho desenvolvido neste estágio foi realizado no âmbito desta intervenção da Deloitte e decorreu, tanto nos escritórios desta operadora de telecomunicações em Angola, como nos escritórios da Deloitte em Portugal.

Este estágio foi realizado em duas fases. Na primeira procedeu-se à:

- Familiarização com o negócio da operadora, com os seus sistemas de informação e ainda com o trabalho realizado por outras equipas da Deloitte em intervenções prévias, nesta operadora;
- Execução de um conjunto de testes, previamente definidos pela outra equipa da Deloitte, nas já referidas intervenções anteriores, cujo objetivo foi identificar perdas na receita e simultaneamente demos formação à equipa da operadora, com o objetivo desta alcançar a sua autonomia na realização destes testes.

No decorrer desta primeira fase foram identificados problemas graves nos sistemas de faturação.

A segunda fase do estágio foi inteiramente direcionada para estes sistemas de faturação devido aos problemas detetados na primeira fase e já referidos. Em particular, na análise do processo de faturação e sistemas de informação subjacentes, na identificação de riscos de segurança de informação desses sistemas, na especificação dos objetivos de controlo e atividades de controlo, no desenho e implementação dos testes relativos a essas atividades. Este processo terminou com a elaboração de um relatório de conclusões, que inclui ainda um conjunto de recomendações e oportunidades de melhoria identificadas.

1.2. Objetivos

O estágio realizado na Deloitte teve como finalidade a participação num trabalho efetivo junto dos clientes na área de risco e *compliance*, realizando o planeamento e a execução de projetos de avaliação do ambiente de controlo dos SI/TI, do risco de segurança de informação e de organização de referência no mercado. No entanto, atendendo ao impacto e criticidade do output do trabalho, a participação neste projeto, exigiu a integração numa equipa com senioridade e supervisão adequadas, passando por compreender/ adquirir e pôr em prática, não só, um conjunto de competências técnicas, mas também de competências comportamentais.

Assim sendo, este estágio teve os seguintes objetivos principais:

- Contacto com a equipa de trabalho e a sua organização;
- Compreensão do âmbito e das metodologias do trabalho;
- Planeamento e organização do trabalho;
- Definição de requisitos/objetivos da avaliação;
- Desenho e caracterização dos testes e procedimentos de avaliação;
- Execução dos testes e procedimentos de avaliação;
- Análise, sistematização e avaliação das conclusões;
- Avaliação dos impactos para a organização;
- Apresentação das conclusões; e
- Preparação do relatório final.

Objetivos do trabalho desenvolvido

A finalidade do trabalho desenvolvido foi ajudar a operadora a compreender os riscos de segurança de informação, decorrentes da falta de controlo sobre os seus SI/TI, nomeadamente na correta captação da receita e controlo da mesma. A necessidade de avaliação dos riscos de SI/TI deve-se ao facto de todas as informações financeiras serem guardadas em SI/TI. Assim, o trabalho de realizado passou por, entre outros:

- Avaliar os controlos realizados aos sistemas de informação da operadora;
- Verificar se existem procedimentos aprovados e se os sistemas de informação estão adequados;
- Verificar se a informação é acedida apenas a pessoas devidamente autorizadas;
- Verificar se a informação está sempre disponível e atualizada;
- Verificar se existem controlos internos relativos ao processamento da informação, permitindo o registo;
- Identificar os riscos aos SI/TI;
- Definir objetivos de controlo e respetivas atividades de controlo;
- Executar testes e procedimentos de avaliação;
- Emitir conclusões do trabalho; e
- Identificar oportunidades de melhoria aos controlos de SI/TI.

Por exemplo a lei de *Sarbanes-Oxley* (SOX) [2], obriga que os sistemas de informação sejam avaliados de forma a garantir que estes não afetam as informações financeiras. Esta lei é aplicável nos EUA, no entanto pelo seu aparecimento nasceu um "movimento" generalizado de melhoria da segurança dos SI/TI em todo o mundo. Mesmo empresas do resto do mundo que não estão sujeitas à lei de SOX, estão a implementar práticas que se aproximam da *compliance* da SOX de forma a criar mecanismos de auditora e segurança confiáveis.

No final do trabalho a operadora terá conclusões e recomendações para implementar, por forma a diminuir os riscos associados à captação da receita.

1.3. Planeamento

Na Imagem 1 encontra-se o Diagrama de *Gantt,* que tem por objetivo expor o planeamento do trabalho geral estipulado para o desenvolvimento do projeto.

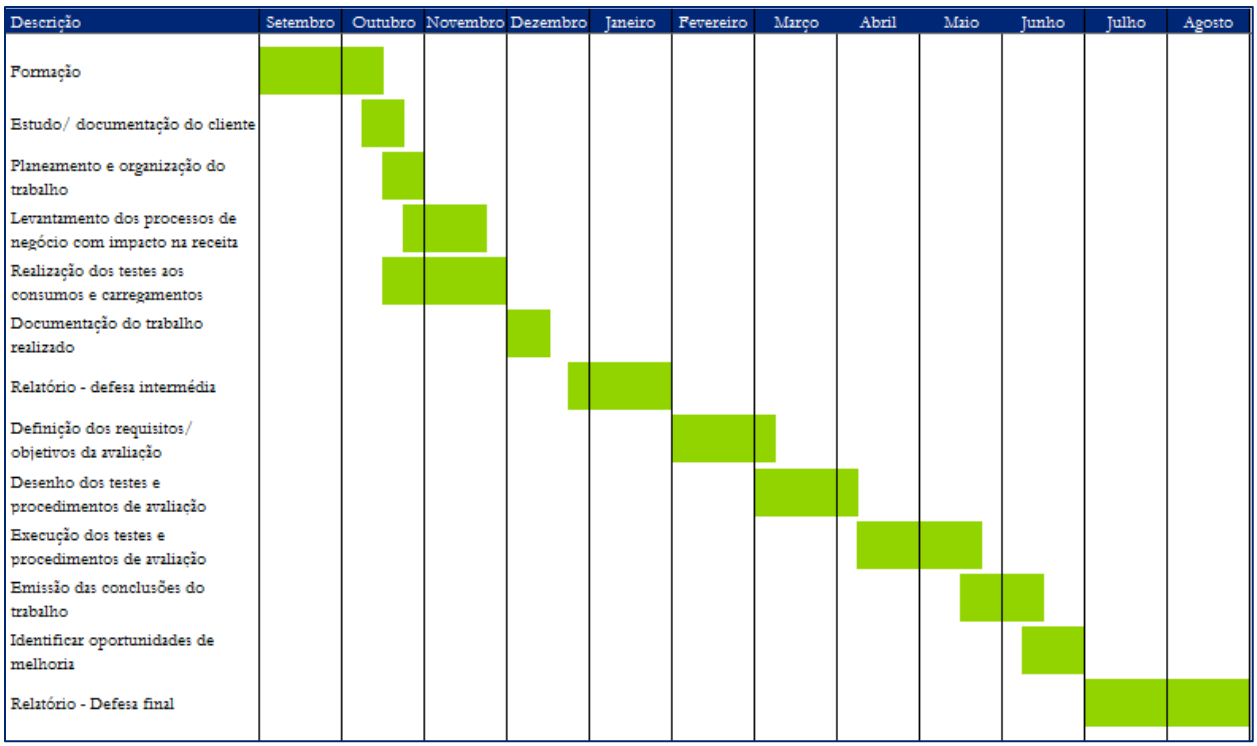

Imagem 1 - Planeamento do trabalho

1.4. Estrutura do relatório

O presente relatório estrutura-se em 5 capítulos principais.

O primeiro corresponde à contextualização global do trabalho, descrição dos objetivos quer do estágio, quer do trabalho, e apresentação do planeamento global do estágio.

No segundo capítulo é apresentada a empresa onde decorreu o estágio, bem como as ações de formação que foram realizadas, durante o primeiro período do estágio.

No terceiro capítulo são apresentadas as noções de base fundamentais à compreensão do trabalho realizado neste estágio, bem como as metodologias *standard*, metodologias proprietárias da Deloitte e as ferramentas necessárias para a elaboração do mesmo. São analisados, o CObIT, as normas ISO/ IEC 27001 e 22301, ITIL - *Incident Managment*, *Risk Intelligence Map* (RIM), *Risk and Control Knowledgebase* (RACK) e para terminar as ferramentas *Audit Command Language* (ACL) e *AuditSystem* 2 (AS/2).

O quarto capítulo incide no trabalho elaborado para a operadora. Neste capítulo revemos os objetivos do trabalho, apresentamos a metodologia utilizada e a abordagem de trabalho, e

descrevemos a equipa. De seguida, é descrito o trabalho que foi realizado na operadora, nomeadamente: o levantamento da realidade, os SI/ TI avaliados, o fluxo de integração da informação, identificação dos riscos, objetivos e atividades de controlo, os testes realizados, as conclusões dos testes e as oportunidades de melhoria.

No quinto e último capítulo sumarizamos as conclusões globais do trabalho realizado ao longo do estágio.

2. Estágio

Este capítulo apresenta a empresa que acolheu a realização do presente estágio. Adicionalmente são referidas todas as formações realizadas no primeiro mês.

2.1. Deloitte

A Deloitte é uma empresa que presta auditoria, consultoria fiscal, consultoria, *corporate finance* e *outsourcing* a cerca de 80% das maiores empresas mundiais. Foi fundada em Londres em 1845, por William Welch Deloitte. Atualmente é uma das maiores organizações de prestação de serviços profissionais em todo o mundo, contando com cerca de 200.000 profissionais.

O primeiro escritório da Deloitte Portugal foi criado em 1968, sob a marca "Deloitte Haskins & Sells". A Deloitte Portugal conta hoje com 1.800 profissionais com escritórios em Lisboa, Porto, e Luanda.

O Departamento de *Enterprise Risk Services*(ERS) da Deloitte, em Lisboa, realiza trabalho de auditoria informática e segurança, ajudando os seus clientes a identificar e a gerir os riscos de negócio associados aos sistemas de informação e a melhorar a utilização da tecnologia.

A missão do departamento de ERS é ajudar os seus clientes a compreender as áreas de risco, que podem afetar o seu negócio na área TMT - aquelas incluem os controlos, processos, e operações de SI/TI - realizando assim a ponte entre os riscos de SI/TI e os do negócio. Nas avaliações dos riscos de SI/TI são usadas metodologias de riscos internas da Deloitte, bem como metodologias *standard* como o CobIT, ITIL, ISO/ IEC 27001 e 22301. É nesta área que o atual estágio é desenvolvido, sob a coorientação local do *senior manager*, Miguel Barão da Cunha.

2.2. Formação

Na Deloitte, sempre que é admitido um novo funcionário, o seu primeiro mês de trabalho é realizado em formações. O período de formação é composto por três fases:

- A primeira fase é composta de formações de boas práticas comportamentais, morais e éticas. Ainda nesta formação os novos profissionais, ficam a conhecer todas as áreas em que a Deloitte trabalha e que valores fornecemos aos nossos clientes;
- A segunda fase foi composta por formações *online*, denominadas como *e-learnings*. Também estas formações são compostas por duas fases. A primeira fase é composta por formações de ética, independência, segurança e confidencialidade para todos os

novos elementos. A segunda fase foi composta por formações específicas para Auditoria, onde foram realizadas formações sobre metodologias e ferramentas; e

- A última fase foi composta por formações apenas direcionadas para o departamento de ERS. A formação foi composta pela explicação de todas as metodologias realizadas no departamento de ERS, bem como realização de exercícios para um cliente fictício.

A Deloitte ainda dispõe de um leque de formações *online* sobre diversos temas que podem ajudar na execução dos trabalhos desenvolvidos. Adicionalmente, contêm uma biblioteca *online* onde os profissionais podem pesquisar em livros e trabalhos já realizados de forma a auxiliar a execução dos projetos e desafios que são apresentados diariamente.

3. Estado da Arte

Este capítulo apresenta as metodologias *standard* e normas de segurança de informação e gestão de risco, bem como metodologias Deloitte, e ferramentas necessárias fundamentais à compreensão do trabalho realizado neste estágio.

3.1. Normas de Segurança de Informação e Gestão de Risco

Na presente secção são descritas as metodologias CObIT, ITIL, ISO/ IEC 27001 e ISO 22301, de forma a fazer a ponte entre as metodologias *standard* de segurança de informação e gestão de risco e o trabalho realizado.

3.1.1. CObIT

O CobIT (*Control Objectives for Information andrelated Technology*) é um guia de boas práticas apresentado como *framework*. Sendo mantido pelo ISACA (*Information System Auditand Control Association*), o CObIT contém vários recursos, que podem servir como modelo de referência para a gestão de TI. É baseado num modelo, que aborda a Gestão de Sistemas de Informação a partir de três dimensões principais: Processos de TI, Recursos de TI e Requisitos de negócio, tal como é mostrado na Imagem 2.

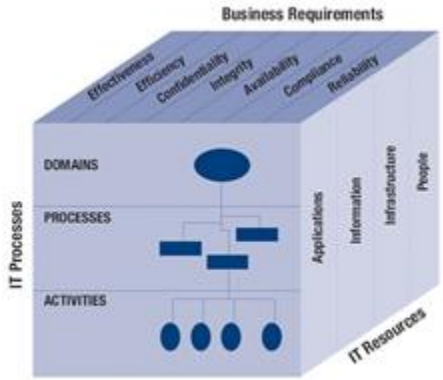

Imagem 2 - Cubo CObIT

Com o CObIT é possível ajudar as administrações a construir uma ligação entre os riscos do negócio e os controlos necessários ao negócio, bem como, os aspetos tecnológicos necessários.

A *framework* CObIT descreve o ciclo de vida de TI com a ajuda dos quatro domínios seguintes:

- Planeamento e Organização: que fornece a direção para a aquisição e implementação de soluções e a respetiva entrega e suporte; sendo composto por 10 processos de negócio;
- Aquisição e Implementação: que fornece soluções de acordo com a direção definida; sendo composto por 7 processos de negócio;
- Entrega e Suporte: recebe soluções para serem transformadas em serviços disponíveis para a organização, bem como para os seus colaboradores; sendo composto por 4 processos de negócio; e
- Monitorização e Avaliação: monitoriza os processos para assegurar que a direção definida é seguida; sendo composto por 13 processos de negócio.

A Imagem 3 apresenta os domínios que foram explicados nos pontos anteriores:

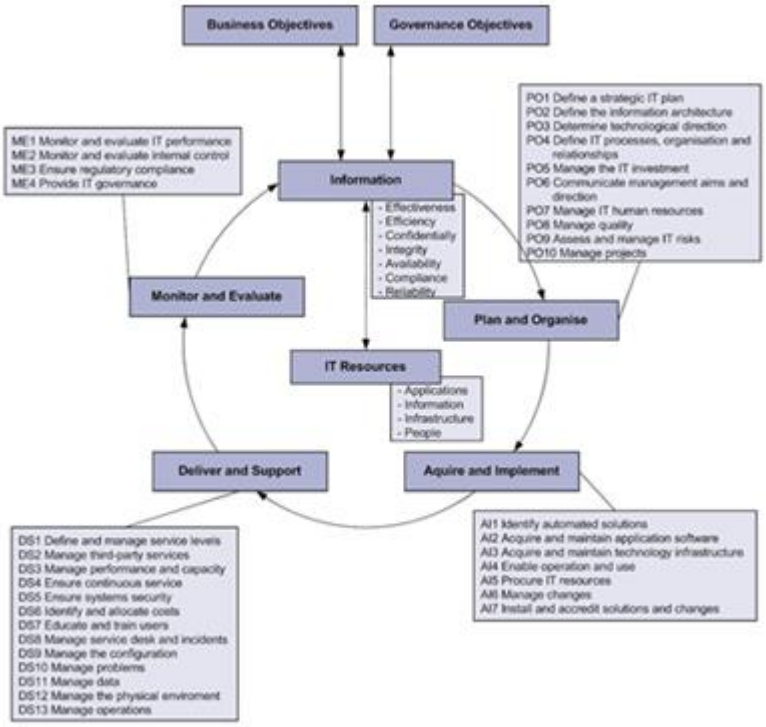

Imagem 3 - Domínios CObIT

O CObIT fornece 34 processos de negócio, para processos de TI, sendo que, esta estrutura abrange todos os aspetos tecnológicos e de informação. Cada processo de negócio é subdividido numa lista de 318 objetos de controlo mais detalhados. Em seguida, é mostrado um exemplo de um processo de negócio subdividido em objetivos de controlo:

Processo de negócio: PO9 - avaliação e gestão de riscos de TI

Este processo permite obter controlo sobre a gestão risco de TI. Este processo oferece estratégias e mitigação de riscos residuais. As estratégias de mitigação dos riscos são adotadas pela organização com objetivo de diminuir o risco. O resultado da avaliação é validado por ambas as partes interessadas, de forma a mitigar o risco detetado para trazer para valor para a organização, a nível financeiro. Estas estratégias englobam:

- *Framework* de gestão de riscos de TI;
- Contextualização do risco;
- Identificação de eventos;
- Avaliação dos riscos;
- Resposta do risco; e
- Manutenção e monitorização de um plano de gestão de risco.

3.1.2. ISO/ IEC 27001

A norma 27001 foi publicada em Outubro de 2005 pela *International Organization for Standardization* (ISO) e pela *International Electrotechnical Commission* (IEC).
Dentro do contexto dos riscos de informação nasce esta norma, de modo a especificar os requisitos para o estabelecimento, implementação, operacionalidade, revisão, manutenção e melhoria de um Sistema de Gestão de Segurança de Informação (SGSI).

As organizações que adotam a norma 27001 conseguem focar-se mais nas necessidades do negócio e considerar a segurança de informação como parte integrante dos objetivos de negócio para realizar a gestão dos riscos.
Devido à utilização cada vez maior das TI existe a necessidade de melhorar a segurança de informação, pois a perceção do risco consequentemente aumenta.

A norma 27001 é composta por duas fases distintas:

Fase 1 - Definição de regras e requisitos de cumprimento da norma, envolvendo os seguintes componentes:

- Contexto de organização;
- Liderança:
  - Liderança e compromisso;
  - Política; e
  - Funções e responsabilidades.
- Planeamento:
  - Ações para endereçar riscos e oportunidades:
    - Avaliação dos riscos de SI; e
    - Tratamento dos riscos de SI.

    - Planeamento de segurança da informação e planeamento para os alcançar.
- Suporte:
    - Recursos;
    - Competências;
    - Consciencialização;
    - Comunicação; e
    - Informação devidamente documentada.
- Operação:
    - Planeamento e controlo operacional;
    - Avaliação de risco; e
    - Tratamento de risco.
- Avaliação de desempenho:
    - Auditoria interna; e
    - Monitorização, mediação, análise e avaliação.
- Melhoria:
    - Em situações de não conformidade, realizar ações corretivas; e
    - Melhoria contínua.

Fase 2 – Implementação de um conjunto de objetivos de controlo que a norma 27001 propõe para as organizações adotarem. Os objetivos de controlo encontram-se documentados no Anexo, que a norma 27001 disponibiliza. A Imagem 4 apresenta os conjuntos de controlo, que as organizações podem adotar:

- A.5 - Politicas de Segurança
- A.6 - Organização da informação
- A.7 - Segurança de Recursos Humanos
- A.8 - Gestão de bens
- A.9 - Controlo de Acessos
- A.10 - Criptografia
- A.11 - Segurança física e ambiental
- A.12 - Segurança de Operações
- A.13 - Segurança de comunicações
- A.14 - Aquisição, desenvolvimento e manutenção de sistemas
- A.15 - Relação com fornecedores
- A.16 - Gestão de incidentes de segurança de informação
- A.17 - Aspetos de SI na gestão da continuidade de negócio
- A.18 - Conformidade

Imagem 4 - ISO 27001

A gestão da segurança de informação deve ser realizada a partir das medidas de controlo sugeridas pela norma, a partir do modelo de processos *Plan – Do – Chek – Act* **(**PDCA), bem como do modelo de análise, avaliação e tratamento de riscos.

Modelo - PDCA

O modelo PDCA baseia-se na implementação do controlo dos processos e da verificação dos sistemas de informação, e é originário da estratégia de administração denominada por *Total Quality Management* (TQM). No âmbito do presente estágio consideramos uma versão do PDCA orientada para a gestão de risco.

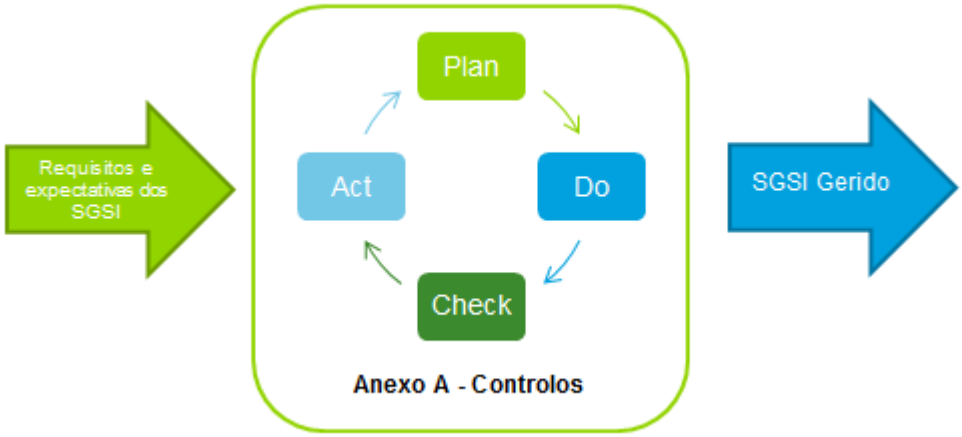

Imagem 5 - PDCA - 27001

- **Plan** (planear): Definição de procedimentos, políticas, processos e objetivos necessários para a administração dos riscos, de modo a aumentar a segurança da informação;
- **Do**(fazer; implementar; e operar): Implementar e operar as políticas, processos e procedimentos que foram definidos na fase de planeamento;
- ***Check*** (verificar; monitorizar; e rever): Monitorização da performance dos processos implementados com as políticas e objetivos definidos; e
- ***Act*** (agir; manter; e otimizar): Realizar medidas corretivas e preventivas, baseadas na monitorização realizada na fase *check*.

Análise e avaliação de Risco

$$\boldsymbol{Risco} = \frac{\boldsymbol{Ameaças} * \boldsymbol{Vulnerabilidades} * \boldsymbol{Impactos}}{\boldsymbol{Medidas\ de\ Segurança}}$$

A avaliação dos riscos é um dos aspetos mais importantes da norma 27001. A avaliação do risco deverá ser realizada inicialmente com a identificação dos riscos, seguida de uma classificação da sua gravidade, de modo a que sejam implementadas medidas de mitigação.
Após a análise dos riscos, torna-se necessário direcionar e determinar quais as ações de controlo apropriadas para a gestão desses riscos. A avaliação dos riscos deve ser determinada tendo em conta uma análise de custo-benefício, pois só depois desta análise é que se

consegue determinar se compensa minimizar ou transferir o risco. Isto é, quando um risco tem uma probabilidade baixa de ocorrer e o seu custo de tratamento é elevado, talvez não compense mitigar esses riscos, ao invés do que acontece com uma probabilidade mais elevada.

Tratamento do risco:
Quando a análise dos riscos se encontra determinada, existe um leque de opções para o seu tratamento:

- Aceitar o risco: A organização tem consciência que o risco existe, sabendo que a política da organização está atenta;
- Evitar o risco: A organização tem consciência do risco, por isso não permite que sejam efetuadas ações que possam sequer causar a ocorrência desse risco;
- Aplicar medidas de segurança: A organização aplica medidas de modo a diminuir os riscos; e
- Transferir o risco: A organização transfere os riscos associados para outras partes (e.g. seguradoras, fornecedores).

3.1.3. ISO/ IEC 22301

A primeira norma internacional a nível mundial para a *Business Continuity Management* (BCM), foi a ISO 22301 Foi desenvolvida com o intuito de ajudar a minimizar o risco associado a acontecimentos disruptivos, para Sistemas de Gestão de Continuidade de Negócio (SGCN). [3] [4]

A norma ISO 22301 especifica os requisitos para estabelecer, planear, realizar, monitorizar, rever, manter e melhorar continuamente um sistema de gestão de modo a prepará-lo para responder e recuperar se tais ameaças realmente ocorrerem. Os requisitos desta norma são genéricos, ou seja, são aplicáveis a qualquer tipo de organização, independentemente do seu tipo, dimensão e natureza.

A partir da norma 22301 a normalização da continuidade de negócio evolui, acrescentando os seguintes benefícios à organização:

- A definição dos objetivos, monitorização do desempenho e métricas são realizadas com mais cuidado;
- A equipa de gestão tem as expectativas mais claras e determinadas; e
- O planeamento e a preparação dos recursos são realizados com mais cuidado de modo a garantir a continuidade de negócio.

A norma ISO 22301 também adota o modelo PDCA. A Imagem 6 ilustra como um Sistema de Gestão de Continuidade do Negócio (SGCN) considera como entradas as partes

interessadas e os requisitos de continuidade de negócio, produzindo como saída a garantia da gestão da continuidade do negócio, através da execução das ações necessárias para atingir os resultados de continuidade desejáveis.

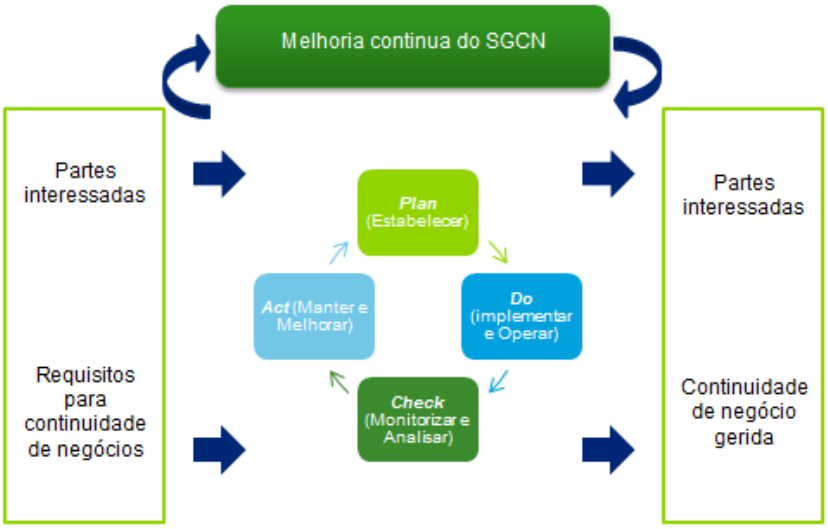

Imagem 6 - PDCA 22301

A norma ISO 22301 é composta por várias cláusulas, sendo que, a aplicação do modelo PDCA reflete-se nas cláusulas 4 a 10, envolvendo os seguintes componentes:

Contexto da organização (cláusula 4)

Para atingir os resultados dos Sistemas de Gestão de Continuidade do Negócio é necessário determinar os requisitos internos e externos. Os requisitos podem incidir nos seguintes pontos:

- Atividades, funções, serviços, produtos ou fornecedores;
- Políticas de continuidade de negócio;
- Objetivos da organização;
- Quantidade de riscos associados à organização; e
- Requisitos legais aplicáveis, regulamentares e outros requisitos que a organização subescreva.

Liderança (cláusula 5)

Para que o SGCN seja bem-sucedido é necessário, que a gestão de topo esteja pronta a liderar e a tomar decisões, de modo a encaminhar a organização a atingir os objetivos. A gestão de topo é responsável por 1) garantir que o SGCN é compatível com a organização; 2) integrar, fornecer e comunicar as medidas necessárias para a sua aplicação; e 3) no final

assegurar que os objetivos são atingidos, bem como a correta atribuição das responsabilidades a cada colaborador.

Planeamento (cláusula 6)

Esta fase estabelece os objetivos necessários para mitigar os riscos associados à organização. É necessário que os objetivos de um SGCN sejam devidamente implementados, para assim ser possível mitigar os riscos, bem como cumprir os requisitos das organizações. Nesta fase também é realizada a avaliação dos riscos, bem como o seu nível de impacto, para que a determinação dos objetivos seja direcionada para mitigar os riscos com maior impacto para a organização.

Suporte (cláusula 7)

A fase de suporte tem como objetivo principal suportar as operações do SGCN, de modo a ajudar a organização a utilizar os recursos necessários e apropriados a cada tarefa. Os recursos devem incluir equipas com as competências necessárias, com uma boa comunicação e sensibilização para a realização de cada tarefa, sendo que, cada uma deve-se encontrar devidamente documentada.
Nesta fase também devem ser consideradas as comunicações internas e externas à organização, devendo estas ser realizadas no momento adequado de forma a adicionarem valor.

Operação (cláusula 8)

Depois do planeamento do SGCN, a organização está em condições para colocar todo o trabalho planeado em funcionamento. Esta fase inclui:

- Análise de Impacto de Negócio (AIN): auxilia a organização a identificar os processos críticos, que suportam os seus principais produtos e serviços, as interdependências entre os processos e os recursos necessários para que a organização funcione pelo menos com os requisitos mínimos;
- Avaliação de Risco: realiza-se recorrendo à norma ISO 31000. A avaliação do risco tem como objetivo estabelecer, implementar e manter um processo formal e devidamente documentado da avaliação do risco. Através deste processo é possível analisar e avaliar quais os riscos mais críticos para a organização.
- Definição de estratégias de continuidade de negócio: depois da realização das duas etapas anteriores, é agora possível desenvolver as estratégias necessárias e determinar mecanismos necessários para recuperar e proteger as atividades mais críticas, ou seja, as que têm um nível de risco mais elevado. As organizações devem ter uma implementação de boas práticas, pois ter uma estratégia global de Gestão de

Continuidade de Negócio (GCN) oferece à organização a garantia que as atividades de GCN estão alinhadas e apoiam a estratégia global de negócios da organização.

- Definição de procedimentos de continuidade de negócio: a documentação dos procedimentos é um ponto-chave para garantir a continuidade das atividades determinadas anteriormente. Estes têm de cumprir os seguintes pressupostos:
    - Ter um protocolo interno e externo de modo a estabelecerem a comunicação;
    - As medidas têm de ser específicas para que, quando for necessário realizar uma interrupção, estas sejam adequadas;
    - Têm de ser direcionados aos impactos que a organização possa sofrer por via de eventos ocorridos, no caso de ser necessário interromper operações;
    - Têm de ser eficientes, de modo a minimizar as consequências da implementação de estratégias de mitigação de risco.
- Desenvolver e testar: de modo a garantir que os procedimentos determinados no ponto anterior estão consistentes com os objetivos de continuidade de negócio, é necessário testá-los regularmente. Só assim é possível assegurar que as estratégias estão a dar repostas e resultados de recuperação.

Avaliação de desempenho (cláusula 9)

Após a implementação da ISO 22301, é agora necessário estabelecer um acompanhamento contínuo, realizando revisões periódicas de modo a melhorar cada vez mais o seu funcionamento. Nesta fase é necessário garantir que:

- A gestão de topo deve assegurar, que todas as metas e os objetivos estão a ser devidamente cumpridos, bem como monitorizar o cumprimento da norma e os objetivos de continuidade de negócio;
- Determinar se o desempenho dos processos, procedimentos e funções estão a ir de encontro com as atividades mais prioritárias;
- Realizar auditorias internas em intervalos planeados; e
- Por fim, avaliar se as atividades foram realizadas dentro do planeado.

Melhoria (cláusula 10)

A melhoria contínua tem de ser realizada com o esforço de toda a organização de forma a continuar a aumentar a eficácia (atingir os objetivos) e a eficiência (uma relação custo/ benefício) dos processos e dos controlos. Todos os dias a organização tem o dever de continuar a exercer uma política de contiguidade de negócio, para cumprir todos os objetivos, de modo a alcançar os resultados esperados.

3.1.4. ITIL –*Incident Management*

O *Incident Management* (IM) do ITIL é um processo desenhado para restaurar o normal funcionamento dos serviços o mais breve possível, de modo a minimizar o impacto dos incidentes sobre as operações de negócio. O IM passa pelas seguintes fases que serão apresentadas de seguida:

- **Identificação:** a organização deve sempre tentar controlar ao máximo todos os componentes importantes, para que falhas ou possíveis falhas sejam detetadas o mais cedo possível, para que o processo de mitigação seja iniciado o mais rápido possível. Numa situação ideal, os incidentes são resolvidos antes de chegarem ao utilizador;
- **Registo:** estando os incidentes identificados, estes têm de ser todos registados, incluindo data e hora. O registo de todos os incidentes ocorridos na empresa, é necessário para garantir um registo histórico;
- **Classificação:** depois dos incidentes estarem registados é necessário ver a quantidade de incidentes e classificá-los como incompletos, incorretos ou extraviado;
- **Priorização:** outro aspeto importante para cada incidente é acompanhá-lo com um código de prioridade, sendo geralmente determinado através da sua urgência e impacto;
- **Diagnóstico:** neste ponto agora é necessário ver os incidentes com priorização maior e realizar um diagnóstico para perceber o que aconteceu para aquele incidente ter ocorrido;
- **Escalamento:** passar a o incidente para outra pessoa/grupo dentro da empresa com competências mais adequadas para a sua resolução. Existem dois tipos de escalamento, sendo estes os seguintes:
    - **Funcional:** passar o incidente para equipas técnicas com *know-how* especializado se este for necessário para a resolução do incidente;
    - **Hierárquico:** notificar os responsáveis hierárquicos do incidente, quando a resolução deste requer autorizações especiais ou poder de decisão mais elevado na hierarquia;
- **Investigação e diagnóstico:** cada grupo investiga os erros ocorridos, para que tal incidente tivesse ocorrido, sendo necessário também aqui realizar um diagnóstico, para garantir uma visão completa de todas as atividades. Se uma solução for identificada, esta deve ser implementada, depois de devidamente testada;

- **Resolução e recuperação:** por vezes pode ser necessário pedir aos colaboradores para realizarem operações específicas no seu departamento. Sendo agora possível implementar uma solução; e
- **Fecho:** quando todas ações de resolução e recuperação estiverem terminadas o incidente pode ser fechado, sendo necessário verificar se todos os utilizadores se encontram satisfeitos. [3] [4]

3.1.5. Matriz de Risco

A matriz de risco teve origem a partir da matriz de Eisenhower, que é uma metodologia para auxiliar na gestão de tempo, de modo a aumentar a eficácia, a eficiência ou produtividade. Para que isso aconteça é necessário compreender a diferença entre as atividades, que são importantes e as que são urgentes. Sendo as atividades importantes o resultado que leva a obtenção dos seus objetivos (profissionais e pessoais) e as atividades urgentes são aquelas que requerem uma atenção imediata e estão, frequentemente associadas à obtenção de objetivos. [5]

Relativamente aos tipos de risco, na perspetiva de Gestão e/ ou Auditoria, podem ser classificados em três tipos:

- **Risco potencial:** possibilidade do aparecimento de um determinado acontecimento que provoque prejuízos materiais ou imateriais, para uma empresa;
- **Risco Inerente:** risco que se encontra sempre associado a alguma transação ou ato de gestão. Neste risco podem ocorrer distorções materialmente relevantes; e
- **Risco Residual:** resulta da associação entre o risco potencial já referenciado e a robustez do controlo, diminuindo esse risco potencial.

A classificação dos riscos serve-se da matriz de risco, como uma ferramenta destinada a avaliar os riscos. Através desta matriz o risco é medido segundo dois vetores:

- Impacto: avaliação das consequências do risco, nos objetivos de um determinado processo;
- Probabilidade: avaliação da probabilidade de ocorrência de risco.

Através da matriz de risco é possível, como já foi referido anteriormente, avaliar o risco, tendo esta três níveis de aceitação, representados na Imagem 7 pelas cores verde (risco aceitável, sem necessidade de intervenção), amarelo (risco médio, com necessidade de supervisão) e vermelho (risco alto, com necessidade urgente de intervenção).

Na Imagem 8 pode verificar-se que a matriz de riscos também se aplica a processos ou projetos específicos, com a finalidade de reduzir o risco para um nível aceitável, havendo para isso a necessidade de uma intervenção permanente.

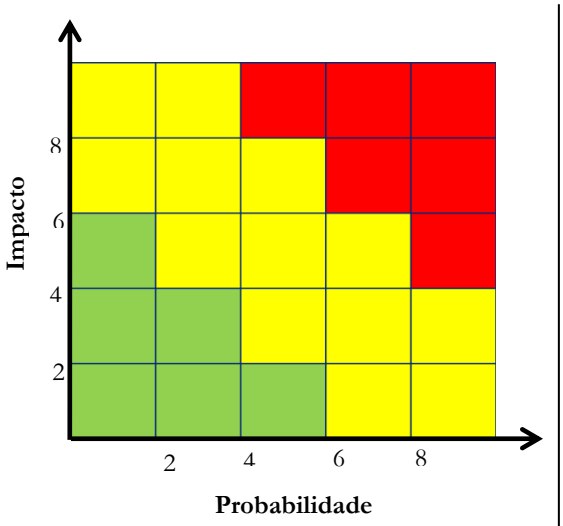

Imagem 7 - Níveis da matriz de risco

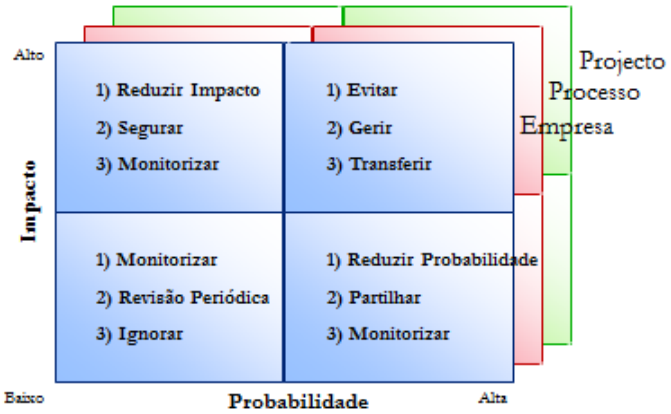

Imagem 8 - Ações da matriz de risco

Esta metodologia para gestão de riscos segue o processo ilustrado abaixo, produzindo e utilizando a matriz de riscos dos processos:

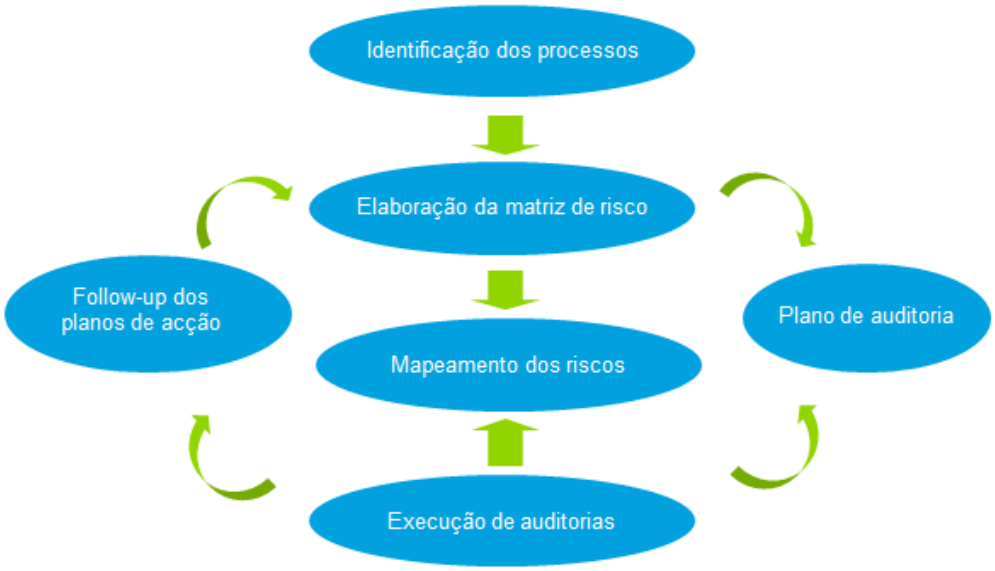

Imagem 9 - Etapas da aplicação da matriz de risco

As etapas para aplicação da matriz de risco são as seguintes:

- Identificação dos processos: nesta fase é necessário identificar/ levantar todos os processos e respetivos fluxos de atividades;
- Mapeamento dos riscos: nesta fase são representados todos os riscos que foram identificados tal como a sua definição, tendo como finalidade classificar os riscos consoante o seu impacto e probabilidade. Aqui também são identificados os *stakeholders* envolvidos nos riscos que foram anteriormente identificados;
- Matriz de riscos: é elaborada com base no dicionário de riscos, sendo aplicada aos processos;
- Plano de auditoria: para a realização deste plano é necessário fazer o levantamento dos pontos identificados nos riscos; identificando os riscos com necessidade de serem auditados e respetivos recursos a utilizar; definir um plano de trabalho; definindo as prioridades tendo em conta o cumprimento das expectativas da Gestão; finalmente, incluir comentários dos operacionais;
- Execução de auditoria: determinar a efetividade operacional das atividades, processos, procedimentos ou controlos existentes com vista à mitigação dos riscos identificados, e da necessidade de reforçar o ambiente de controlo interno através do reforço da efetividade das mesmas, ou mediante a criação de novas atividades, processos, procedimentos ou controlos; e
- *Follow-up* dos planos de ação: definir as prioridades de uma melhor combinação de medidas a tomar, visto que a implementação de todas as medidas de tratamento podem não ser *cost-effective*. A tomada de decisão em relação à implementação de medidas adequadas terá de ter em consideração a redução de níveis de risco para um nível aceitável.

3.2. Metodologias Deloitte

Nesta secção encontram-se descritas as metodologias Deloitte, nomeadamente: *Risk Intelligence Map* (RIM), *Riskand Control Knowledgebase* (RACK) e dos Controlos Gerais Informáticos (CGI) propriedade da Deloitte, que foram utilizadas para a realização do estágio. As metodologias que se apresentam descritas, nesta secção, são consideradas como "aceleradores" e foram desenvolvidas com base nas metodologias apresentadas na secção 3.1 do presente relatório.

3.2.1. Deloitte's Risk Intelligence Map (RIM)

Tal como o nome refere, o RIM é um mapa de risco, propriedade da Deloitte, para auxiliar a identificação correta dos riscos, de forma a abranger todas as áreas possíveis. Este mapa pode ser considerado como um "painel de riscos" ou ferramenta de monitorização (1).

Com esta ferramenta é possível planear possíveis cenários, com o objetivo de identificar os riscos que estão relacionados e os que podem interagir, sendo uma grande vantagem devido

a auxiliar o utilizador deste mapa, a ter uma visão mais abrangente dos riscos que podem ocorrer, mesmo aqueles que só consegue detestar a partir da sua utilização. Vejamo-lo como uma árvore, ou seja, muitas vezes os nós vizinhos fazem todo o sentido serem considerados. O RIM pode ser também considerado como uma ferramenta de estratégia, isto é, ajuda na deteção dos riscos que estão associados a uma única estratégia de negócio e a que iniciativas.

O RIM também pode ser considerado uma ferramenta de avaliação de risco, ou seja, auxilia na deteção de riscos que são relevantes para um certo tipo de empresa/ unidade de negócio/ avaliação funcional dos riscos (e.g. avaliação a partir da matriz de risco). Também é possível identificar riscos relacionados com os funcionários da empresa, ou seja, quais os riscos que estes podem trazer para a empresa ou indústria.
Com o RIM não é possível classificar os riscos, nem mesmo os seus impactos, pois serve apenas como uma ferramenta de ajuda a identificar os riscos que a empresa pode ter, ou ser um ponto de partida para os classificar e gerir de uma forma mais abrangente.

3.2.2. Risk and Control Knowledgebase (RACK)

Antes de falar do RACK é necessário realizar uma breve introdução sobre os Objetivos de controlo e as respetivas atividades de controlo.

3.2.2.1. Objetivos de controlo

Os objetivos de controlo (OC's) são assim designados por definirem as metas que são necessárias alcançar para se conseguir mitigar os riscos que foram identificados. Quando os objetivos de controlo forem alcançados, conseguimos mitigar os riscos.

3.2.2.2. Atividades de controlo

As atividades de controlo (AC's) são tarefas usadas para ajudar a garantir que os objetivos de controlo são alcançados, sendo assim mitigados os riscos (3). As atividades de controlo podem ser de várias formas, entre elas:

- Políticas e procedimentos: são atividades realizadas por colaboradores que implementam um conjunto de regras e contribuem para o bom funcionamento da empresa (e.g. existe uma política e procedimento para o tratamento de existência de contas não pagas);
- Aprovações: atividades realizadas por colaboradores que garantem que a informação é distribuída de forma correta e chega aos cargos superiores de modo a serem aprovadas (e.g. a administração deve aprovar a implementação técnica de novas rotas de interligação);
- Verificações: atividades realizadas por colaboradores de modo a validarem a informação (e.g. são efetuadas validações e verificações pelo sistema, aos dados

introduzidos, referentes a pagamentos e recebimentos de clientes. Erros identificados são corrigidos imediatamente);

- Reconciliações: atividades realizadas por colaboradores de forma a validarem a integridade da informação (e.g. é efetuada a reconciliação diária e/ou mensal dos registos de roaming.);
- Avaliações de desempenho: atividades realizadas pela administração de modo a efetuarem uma avaliação do desempenho dos seus colaboradores (e.g. é realizada uma revisão periódica dos acessos aos sistemas de pedidos de clientes pela gestão, com base nas responsabilidades/ funções dos colaboradores;
- Medidas de segurança: atividades realizadas por colaboradores de modo a que não seja comprometida a segurança da empresa (e.g. todos os colaboradores realizam a autenticação via password nos edifícios); e
- Segregação de funções: atividades que consistem na separação de funções que possam representar conflitos de interesses (e.g. é realizada uma verificação semestral, se existe segregação de funções, entre os indivíduos que mantêm e atualizam o master file do fornecedor e os que processam as contas a pagar e realizam os pagamentos).

O que é o RACK?

O RACK é uma base de dados centralizada, propriedade da Deloitte, contendo os seguintes pontos:

- Objetivos de Controlo (OC's);
- Atividades de Controlo (AC's);
- Testes; e
- Evidências.

O seguinte esquema apresenta todos os componentes para a pesquisa dos OC's e das AC's:

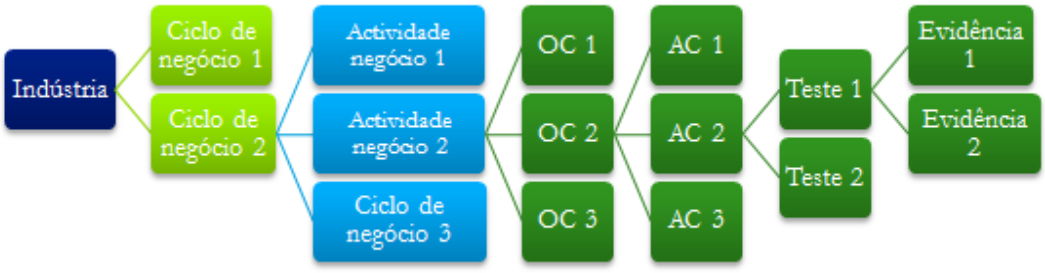

Imagem 10 – Organização RACK

O RACK contém dados sobre cerca de 30 tipos indústrias (e.g. telecomunicações) sendo que estas abrangem todas as indústrias com que a Deloitte interage. Para cada indústria, o RACK tem associados os vários ciclos de negócio (e.g. receita); cada ciclo de

negócio, por sua vez, tem várias atividades de negócio (e.g. roaming); e a cada atividade estão associados os objetivos de controlo (e.g. os registos de roaming são classificados/calculados através de taxas válidas negociadas). A cada objetivo de controlo estão associadas as atividades de controlo (e.g. as alterações às taxas ou novas taxas são aprovadas por pessoal autorizado e enviadas em tempo útil para os sistemas de faturação ou *clearinghouses*), sendo estas utilizadas para alcançar os objetivos de controlo. Por fim, a cada atividade de controlo estão associados os testes para comprovar que as atividades de controlo foram bem implementadas, sendo que, para a execução dos testes são necessárias evidências para a elaboração dos mesmos.

A partir do RACK é possível determinar os objetivos de controlo, e assim garantir que são abrangidos todos os pontos essenciais. No final, apenas temos de filtrar os objetivos de controlo, consoante o negócio em que queiramos incidir.

3.2.3. Controlos Gerais Informáticos

Uma auditoria de Controlos Gerais Informáticos (CGI) é uma auditoria informática, que tem como finalidade identificar e documentar o ambiente de controlo dos sistemas de informação (e.g. SAP) de uma empresa.

Uma auditoria CGI passa pela avaliação do ambiente geral de controlo dos SI, bem como pela realização de um diagnóstico das principais debilidades existentes ao nível dos controlos e dos riscos associados. Estas incidem sobre três áreas principais — Gestão de Operações e CPD, Segurança da Informação, e Gestão de Alterações; sendo que em cada uma delas são analisados quatro tipos de elementos tecnológicos: Aplicações, Bases de Dados, Sistemas Operativos e Redes.

Segundo a metodologia Deloitte, a revisão aos Controlos Gerais Informáticos deverá ser realizada de acordo com a seguinte abordagem:

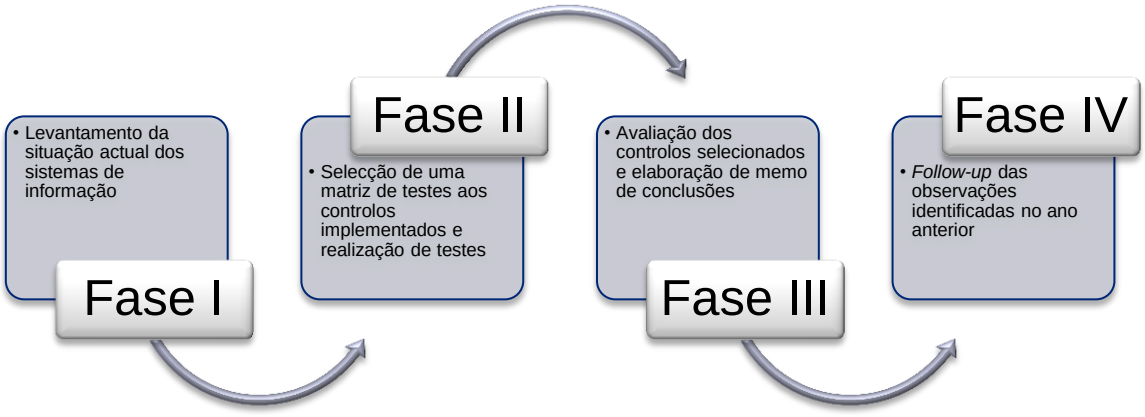

Imagem 11 - Diagrama da metodologia seguida numa auditoria CGI

Fase I

O levantamento e documentação dos riscos de segurança dos SI, de forma a realizar uma auditoria aos sistemas da empresa, sempre que necessário.

Para realizar o entendimento dos SI, é necessário primeiro de entender as subsecções que se seguem, para posteriormente definirem os riscos associados aos riscos de IT (RAITs).

Áreas dos controlos gerais de TI

Esta fase tem como objetivo selecionar o ambiente onde se insere o sistema a avaliar, bem como as áreas que interagem com o sistema. Identificar a existência de empresas prestadoras de serviços externos, que intervêm nas áreas identificadas anteriormente, em regime de *outsourcing* (o regime de *outsourcing*, será explicado nas próximas secções).

Informação do sistema organizacional e pessoal

Esta fase tem como objetivo, compreender como é realizada a gestão dos sistemas de informação utilizados na organização. Conhecer a composição do departamento de sistemas de informação, através de um organograma da empresa.

Caracterização das áreas dos controlos gerais de TI

Na subsecção que se segue estão descritas as áreas que são avaliadas na CGI. As áreas descritas descrevem os detalhes necessários para conhecer todo o ambiente de SI/TI do cliente.

A informação destas áreas é obtida através de uma reunião presencial com o cliente. No final da reunião o Auditor já possui informação suficiente para determinar os riscos de IT (RAITs).

Centro de Processamento de Dados e operações de rede

Levantamento dos procedimentos operacionais do ambiente de processamento da informação em análise, nomeadamente:

- Procedimentos de manutenção e sua formalização;
- Identificação dos *Job's/batch's* e respetiva calendarização; e
- Comunicação e correção dos erros.

Levantamento da arquitetura dos sistemas de *backup*. Para isso, é necessário identificar:

- A pessoa responsável por gerir o sistema de *backups*, bem como, qual a sua função dentro da empresa;
- Quais os tipos de *backups* realizados, assim como, a periodicidade de cada um;
- Qual a rotatividade das tapes;

- Os tipos de acesso ao arquivo físico, as condições da sala (e.g. existência de extintores) e catalogação - esta operação requere uma visita ao Centro de Processamento de Dados (CDP)
- As políticas de segurança de arquivo, nomeadamente se a empresa realiza arquivo para *off-site*. Um arquivo para *off-site,* entende-se por armazenamento dos seus *backups* num sítio a uma distância bastante considerável do edifício que contêm o CPD para que, em caso de catástrofe natural, não existam perdas de informação;
- Existência de um procedimento de *reporting* e correção de erros na realização dos *backups*;
- Existência de relatórios de sucesso da realização dos *backups*;

Caso a empresa possua um serviço de *helpdesk* procede-se à caracterização do seu funcionamento através da identificação:

- dos tipos de problemas que são reportados;
- da quantidade de operadores;
- dos níveis de resolução de problemas; e
- do limite de tempo para a resolução dos pedidos e SLA's (no caso de se tratar de um serviço prestado por um fornecedor externo).

Gestão de acessos

A gestão de acesso está disposta em três grandes áreas que são necessárias avaliar.

a) Políticas, normas e procedimentos de segurança.
   É necessário avaliar:
   - a existência formal de políticas e procedimentos de segurança para o ambiente de processamento da informação em análise;
   - a existência de um programa de divulgação aos colaboradores das políticas, procedimentos e práticas de segurança; e
   - o grau de sensibilidade dos colaboradores relativamente à Segurança.

b) Segurança lógica
   - Identificação dos processos utilizados para restringir o acesso lógico às aplicações e aos dados (SO, rede, aplicação, bases de dados);
   - Indicação do tipo de gestão de controlo de acessos (centralizada/ descentralizada);
   - Identificação do *software* utilizado (SO e aplicações) para restringir o acesso lógico às aplicações e aos dados;
   - Identificação das tecnologias utilizadas para autenticação da identidade dos colaboradores (e.g. *passwords*, cartões magnéticos, dispositivos biométricos);
   - Descrição dos procedimentos para autorização de acessos a dados e atribuição de acessos a utilizadores;

- Existência de acessos externos aos sistemas (e.g. vpn).

c) Segurança física
   - Identificação dos métodos utilizados para restrição do acesso físico ao edifício e CPD (e.g. cartões magnéticos, dispositivos biométricos);
   - Identificação dos grupos de colaboradores com acesso físico ao CPD, nomeadamente:
     - Colaboradores internos: quem são os colaboradores e qual a sua função na empresa;
     - Colaboradores externos: qual a empresa e a razão pela qual necessita de acesso ao CPD; e
     - Outros colaboradores internos e externos sem acesso ao CPD: como é realizado o controlo de acesso no caso de acederem ao CPD.
- Identificação dos tipos de controlos ambientais implementados para prevenção de danos nos equipamentos e informação:
  - Deteção e extinção de incêndios;
  - Monitorização de temperatura e humidade; e
  - Fontes de alimentação alternativas (geradores, UPS's).
- Indicação de:
  - Inexistência de material inflamável;
  - Existência de paredes antifogo (resistentes durante, pelo menos, 6 horas);
  - Existência de extintores manuais;
  - Existência de cablagem devidamente protegida; e
  - Existência de saídas de emergência devidamente assinaladas.

Caracterização da Rede e do Ecossistema de *software*

A caracterização do funcionamento da rede que suporta o ambiente de processamento da informação em análise tem em conta os seguintes pontos:
- Topologia de rede, de modo a entender a disposição de todos os componentes;
- Principais localizações físicas; e
- Funções e responsabilidades da gestão de rede.

A descrição dos procedimentos de aquisição, implementação e manutenção do *software* do aplicacional (e.g. SO) requer:
- Identificar se estão definidos procedimentos para aquisição de novo *software* de suporte (e.g. Microsoft Office Visio, Antivírus);
- Identificar se existem critérios definidos na empresa para selecionar o fornecedor; e
- Identificar se a empresa realiza análise de impacto.

Caracterização da gestão de alterações

Para obter uma descrição detalhada dos processos de gestão de alterações ao *software* e às aplicações da empresa é necessário:

- Identificar os procedimentos de gestão de alterações efetuados pela empresa;
- Identificar se existe aprovação de novas implementações e/ou modificações por parte dos responsáveis;
- Identificar se existe segregação de funções entre as equipas de desenvolvimento, testes e implementação;
- Identificar se existe validação da integridade e exatidão de processamento, após a implementação e/ou modificação;
- Identificar se os testes são aprovados pelos utilizadores do negócio, antes de serem transportados para produção; e
- Identificar se existe documentação de todas as fases do processo.

Caracterização detalhada dos processos de aquisição, implementação e manutenção de aplicações

Nesta fase é necessário compreender como é realizada a aquisição, implementação e manutenção de sistemas aplicacionais, incluindo as funções e responsabilidades de todos os intervenientes no processo. Para isso é necessário identificar:

- O procedimento definido pela empresa para aquisição de novas aplicações (e.g. SAP);
- Critérios de seleção de fornecedores;
- Se são realizadas análises de impacto;
- O procedimento definido pela empresa para aquisição, implementação e manutenção das bases de dados, incluindo as funções e responsabilidades de todos os intervenientes no processo; e
- O procedimento definido pela empresa para gestão de alterações à base de dados.

Identificação de riscos

Nesta componente é necessário identificar os riscos associados às deficiências identificadas ao nível dos procedimentos/ políticas da empresa. Posteriormente os riscos serão avaliados e determinados no memo de conclusões, que será descrito nas próximas secções.

Registo Persistente do Levantamento

No final do levantamento de toda a informação o auditor tem de preencher o formulário da ferramenta AS/2 denominado por "1540 - Understandthe IT

Environment". Este formulário contém todos os campos das subsecções que foram descritas anteriormente. A Imagem 12 ilustra um *screen capture* do formulário.

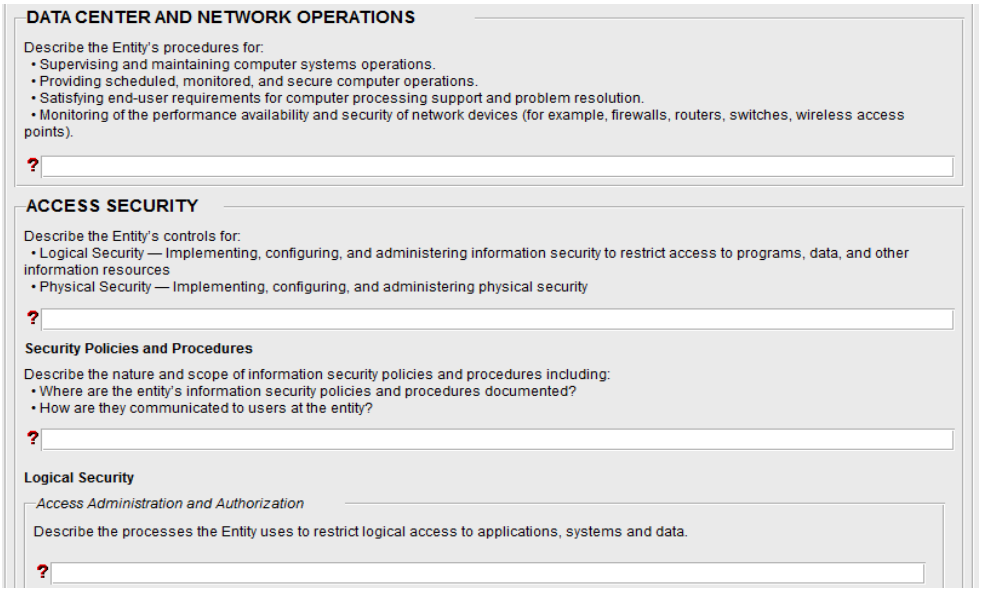

Imagem 12 - Exemplo de preenchimento do formulário 1540

Fase II

A segunda fase da CGI é a realização da matriz de controlo (ou matriz de testes). Estando a Fase I completa, torna-se possível testar o desenho & implementação através da informação obtida, ou seja, verificar se para os testes definidos o cliente possui um procedimento implementado e documentado. No caso de não o ter, é necessário comunicar com o cliente de modo a perceber que controlos estão implementados, para assim serem documentados e avaliados pelos Auditores.

Depois dos testes ao desenho & implementação realizados, é necessário verificar se estes estão realmente a serem implementados na empresa, para isso, realizam-se os testes à operacionalidade. Entende-se por testar/confirmar a operacionalidade quando se realizam testes ao funcionamento/desenho do controlo (e.g. relativamente à realização de backups diários, o teste é obter Logs de backups referentes a uma amostra previamente selecionada).

Naturalmente, antes da realização dos testes, é preciso definir a informação necessária, para isso, define-se uma tabela com pedidos de evidências. Esta tabela é enviada para o cliente, para que este forneça a informação necessária para a realização dos testes. De seguida, segue a explicação de cada pedido realizado ao cliente.

Pedido de informação

Depois da definição dos testes, é necessário determinar toda a informação necessária para a sua realização. Desta forma, solicitamos a informação ao cliente, depois de efetuada uma listagem com os respetivos pedidos de informação, para ser enviada via e-mail ao cliente.

A informação pedida encontra-se organizada da seguinte maneira:

1. Geral: pedidos que são de âmbito geral a toda a organização (e.g. diagrama de rede; organigrama; listagem de colaboradores que abandonaram a empresa em estudo);

Tabela 1 – Pedido de informação geral

ID	Pedido	Descrição
GER.01	Diagrama de Rede	Para realizar uma avaliação a toda a rede, bem como visualizar todos os pontos de segurança que a rede possui (e.g. *firewalls*).
GER.02	Organigrama da organização	O organigrama da organização permite visualizar a estrutura da empresa, bem como a do departamento responsável pelos SI. Por exemplo, para a aprovação de um novo utilizador no sistema, é necessário uma pessoa que ocupe um cargo superior que tenha controlo nos novos colaboradores que acabam de entrar na empresa.
GER.03	Contratos celebrado entre parceiros de negócio.	No caso de haver alguma empresa a realizar prestação de serviços, é necessário pedir o contrato celebrado entre as partes. A avaliação do contrato tem de ser pormenorizada de modo a verificar todas as responsabilidades que o parceiro de negócio tem de cumprir. Adicionalmente, é necessário verificar se o contrato se encontra assinado por ambas as partes bem como se encontra em vigor no ano em âmbito.
GER.04	Listagem de colaboradores que saíram dos quadros da Empresa durante o mês em âmbito.	Listagem dos colaboradores que saíram no mês em âmbito. Para a realização dos testes, é necessário receber do cliente os seguintes dados: (i) Número de colaborador; (ii) Nome; (iii) Data de saída da empresa; (iv) Direção/Área.

2. Gestão de Operações: informação relacionada com as operações que são efetuadas aos sistemas da empresa (e.g. *jobs* dos sistemas, *backups*, *jobs* dos *backups*, entre outros). Na tabela seguinte podemos observar os pedidos que são feitos para realizar a gestão de operações:

Tabela 2 – Pedido de informação gestão de operações

ID	Pedido	Descrição

OP.01	Políticas e procedimentos de gestão de *backups* dos SI em âmbito	Políticas e procedimentos que se encontram implementados pela empresa, para realizarem a gestão de *backups* dos SI em âmbito.
OP.02	Listagem dos *jobs* de *backup* configurados no sistema em âmbito	Listagem de todos os *jobs* realizados pelo SI em âmbito. A partir desta informação é possível saber o tipo de *jobs*, bem como a sua calendarização.
OP.03	*Log* da execução dos *jobs* de *backups* do sistema em âmbito, processados no dia identificado na amostra.	Do universo obtido pela listagem recebida em OP.02, seleciona-se uma amostra. A partir dessa amostra é solicitado os logs de modo a que seja possível analisar a execução dos *jobs* de *backups* e verificar se ocorreram erros.
OP.04	Evidência da monitorização (e.g. relatório) realizada ao processamento dos *backups* do SI em âmbito para a amostra definida.	Para a mesma amostra selecionada em OP.03 é necessário pedir evidências que o cliente realiza monitorização dos backups (e.g. relatório diário com a listagem de jobs realizados com e sem sucesso)
OP.05	Procedimentos de gestão e monitorização dos *jobs*/*batches* dos SI em âmbito.	Este procedimento deverá incluir os processos *job*/*batch* definidos (nomeadamente os de maior criticidade), as normas e orientações relacionadas com a aprovação/calendarização de *jobs*, assim como os procedimentos e responsáveis pela sua monitorização e correção, dependendo do tipo de *jobs* existentes: (i) muito importantes; (ii) importantes; (iii) menos importantes.
OP.06	Listagem dos *jobs*/*batches* configurados no SI em âmbito.	Listagem de todos os *jobs*/*batches* relativamente ao SI em âmbito, bem como a sua calendarização.
OP.07	*Log* dos *jobs*/*batches* do SI em âmbito, processados no dia identificado como amostra.	Do universo obtido da listagem recebida em OP.06, seleciona-se uma amostra de dias. São pedidos os *logs* dos *jobs*/*batches* do SI em âmbito, para a amostra selecionada.
OP.08	Evidência da monitorização realizada ao processamento dos *jobs*/*batches* de operação do SI em âmbito.	Informação de monitorização (e.g. relatório; alertas recebidos) ao processamento dos *jobs*/*batches* de operações do SI em âmbito.
OP.09	Evidência do testes de *restore* das tapes de *backup*.	Informação de testes de *restore* efetuados às tapes de *backups*, bem como a sua calendarização.
OP.10	Plano de Continuidade de Negócio.	Informação de um plano de continuidade de negócio, inclusive um plano de recuperação de desastre.
OP.11	Procedimentos de Gestão de Incidentes e Problemas	Procedimento descrito pela empresa sobre como gerir incidentes e problemas quando estes ocorrem.
OP.12	Matriz de segregação de funções	Matriz com as responsabilidades de cada colaborador da empresa. A separação entre funções de autorização, aprovação de operações, execução, controlo e contabilização, é fundamental para que nenhum colaborador contenha poderes e atribuições em desacordo com este princípio de controlo interno.

3. Segurança de informação: informação relacionada com a segurança de informação, nomeadamente, políticas e procedimentos determinados pela empresa de modo a

que toda a organização cumpra o que está descrito nos procedimentos. Adicionalmente, é necessário pedir informações para comprovar que as políticas e procedimentos estão implementados na empresa. Na tabela seguinte podemos observar os pedidos que são feitos para aferir a segurança de informação:

Tabela 3 - Pedido de informação segurança de informação

ID	Pedido	Descrição
SEG.01	Procedimento de gestão de acessos ao centro de processamento de dados (CPD).	Este procedimento deverá conter as regras de segurança relativamente aos acessos ao CPD.
SEG.02	Política de Segurança de Informação.	Política implementada pela empresa relativamente à segurança de informação.
SEG.03	Procedimentos de gestão de acessos aos sistemas.	Procedimento com descrição da gestão de acessos realizada pela empresa, tais como: procedimentos de criação, alteração, remoção e revisão de acessos.
SEG.04	Política de Gestão de *Passwords*.	Política implementada pela empresa relativamente à gestão das *passwords* (e.g. tamanho mínimo de caracteres).
SEG.05	Procedimento de atribuição de acessos remotos (VPN).	Procedimento com as regras de atribuição de acessos remotos (VPN), ou seja, como é realizado um pedido de acesso, a sua aprovação e atribuição.
SEG.06	Regras de nomenclatura na criação dos utilizadores com acesso ao sistema em âmbito.	Regras que definem uma nomenclatura na criação de utilizadores.
SEG.07	Listagem dos utilizadores e respetivos perfis do sistema em âmbito, em produção.	Listagem de utilizares do sistema em âmbito, com os seguintes parâmetros: userID; Nome de utilizador; Data de criação; e Perfil de acesso. Adicionalmente é necessário informação sobre os perfis do sistema em âmbito.
SEG.08	Evidências do processo de pedido/atribuição de acessos no sistema em âmbito.	Do universo obtido da listagem recebida em SEG.07 seleciona-se uma amostra. Solicita-se à empresa a seguinte informação: - Evidência do Pedido de Criação/Alteração dos acessos; e - Aprovações dos acessos.
SEG.09	Listagem dos utilizadores com acesso à base de dados e respetivos perfis do sistema em âmbito, em produção.	Listagem de utilizares com acesso direto à base de dados do sistema em âmbito, com os seguintes parâmetros: userID; Nome de utilizador; Data de criação; e Perfil de acesso. Adicionalmente é necessário informação sobre os perfis do sistema e a data de criação dos utilizadores do sistema em âmbito.
SEG.10	Evidência (e.g. relatório) da última revisão de acessos realizada no sistema em âmbito.	Informação sobre a última revisão de acessos aos perfis dos utilizadores do sistema em âmbito.
SEG.11	Parâmetros de autenticação à base de dados.	Parâmetros determinados pela empresa, relativamente aos utilizadores da base de dados do sistema em âmbito.

SEG.12	Listagem de utilizadores ativos na *Active Directory*.	Listagem de utilizadores do *Active Directory* incluindo data de criação e respetivos grupos de acesso (nomeadamente *domain admin*).
SEG.13	Informação dos parâmetros de segurança da *Active Directory*.	Evidência (e.g. *print screen*) dos parâmetros de segurança da *Active Directory Password Policies* (e.g. *Password Minimum Length & Complexity, Password Expiration), Account Lockout etc.*

4. Gestão de alterações: informação relacionada com as alterações efetuadas ao sistema em causa, bem como às respetivas bases de dados e sistema operativo. Na tabela seguinte podemos observar os pedidos que são feitos para realizar a gestão de alterações:

Tabela 4 - Pedido de informação gestão de alterações

ID	Pedido	Descrição
ALT.01	Metodologia/ Procedimento de gestão de alterações.	Metodologias/ Procedimentos definidos pela empresa para realizar a gestão de alterações.
ALT.02	Listagem de alterações ao sistema em âmbito.	Listagem de alterações, nomeadamente manutenção evolutiva e corretiva, realizada ao sistema em âmbito (incluindo às BDs), ocorridas no ano em âmbito (com informação da data de início e data de fim).
ALT.03	Listagem de alterações ao SO do sistema em âmbito.	Listagem de alterações (*updates*, instalações de *patches*) no SO de suporte ao sistema em âmbito durante o ano em âmbito (com informação da data de início e data de fim).
ALT.04	Alterações ao sistema em âmbito, relativamente à amostra selecionada.	Do universo obtido da listagem recebida em ALT.02, seleciona-se uma amostra. Para a amostra selecionada, é necessário obter a seguinte informação: - Pedido de alteração; - Aprovação formal da alteração; - Documentação da especificação funcional/ requisitos; - Plano de testes; - Relatórios com resultados dos testes; - Aprovação dos testes de aceitação; e - Pedido e aprovação da passagem a produção.
ALT.05	Alterações ao SO do sistema em âmbito, relativamente à amostra selecionada.	Do universo obtido da listagem recebida em ALT.03, seleciona-se uma amostra. Para a amostra selecionada, é necessário obter a seguinte informação: - Evidência da instalação em qualidade antes de produção - Evidência dos testes/monitorização realizados ao SI de forma a garantir que não teve impacto negativo - Aprovação para instalação em produção.

SELEÇÃO DE AMOSTRAS

Como foi referido anteriormente, para alguns pedidos é necessário selecionar uma amostra. A seleção de amostras pode ser feita por um dos dois tipos descritos a seguir:

Seleção estatística:

- A amostra é selecionada aleatoriamente, ou seja, com auxílio de uma ferramenta de *sampling* que o departamento de ERS utiliza; e
- A distribuição de probabilidades de seleção deve ser uniforme no universo (população) de unidades.

Seleção não estatística:

- A amostra é selecionada através de julgamento profissional;
- Como o objetivo da amostragem é obter conclusões sobre um universo, é necessário, sempre que possível, selecionar uma amostra representativa, através da escolha de itens que tenham as características típicas da população; e
- Sempre que possível, deve selecionar-se de uma forma aleatória, para não existirem julgamentos tendenciosos.

Matriz de Controlo

Os testes são realizados com a informação que foi recebida do cliente, a partir dos pedidos de informação.

A matriz de controlo tem como objetivo auxiliar na avaliação da segurança da informação do sistema em âmbito. A cada objetivo de controlo estão associados vários testes a serem realizados, sendo que para cada um é necessário avaliar os dois itens seguintes:

DESENHO&IMPLEMENTAÇÃO (D&I):

Para a avaliação do desenho & implementação das atividades de controlo deverão ser realizadas as seguintes atividades:

- Descrição dos procedimentos para avaliar o desenho e implementação; e
- Descrição do trabalho realizado para a avaliação do desenho e implementação da atividade de controlo.

OPERACIONALIDADE (OE):

Os testes à operacionalidade são realizados com o objetivo de comprovar que o que está descrito no teste de *D&I* está realmente a ser realizado pelo cliente. É neste ponto que a informação recebida é avaliada e testada, de modo a comprovar que todas as atividades de controlo estão a ser devidamente implementadas.

As conclusões relativamente à efetividade do *desenho & implementação* e *operacionalidade* deverão ser obtidas do seguinte modo:

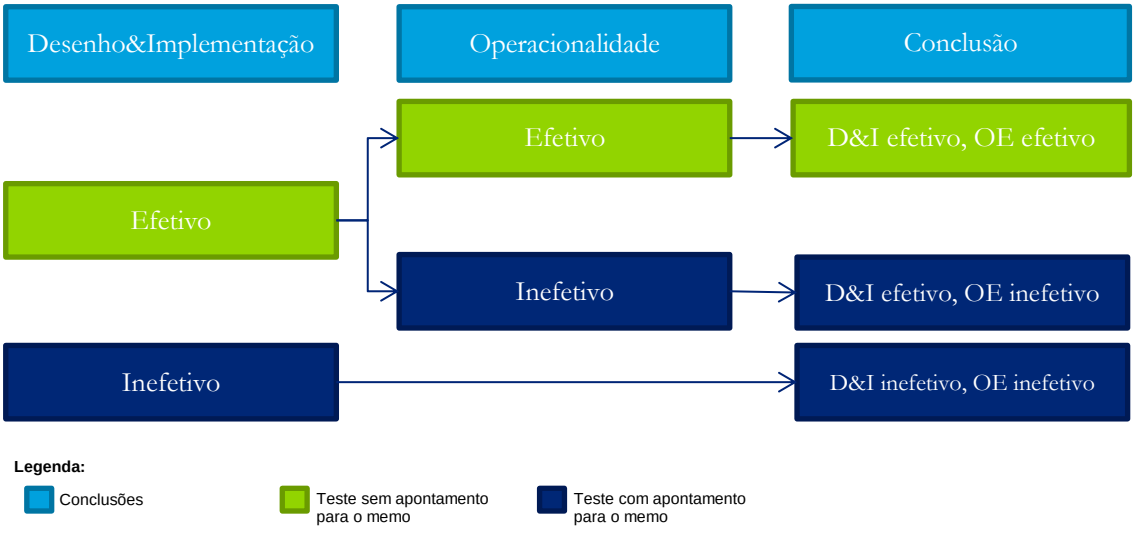

Imagem 13 - Fluxo de conclusões dos testes

Como pode ser observado na Imagem 13,podem existir três tipos de conclusões:

- Teste efetivo no D&I e OE: resultados positivos para o D&I e OE, logo não necessitam de ser reportado para o memo de conclusões;
- Efetivo no D&I e inefetivo na OE: os resultados para o D&I são positivos, no entanto o mesmo não sucedeu com o OE é necessário reportar os problemas detestados; e
- Inefetivo no D&I e na OE: o resultado foi negativo para o D&I e OE, é necessário reportar ambos os casos para o relatório.

Fase III

Memo de Conclusões

O memorando de conclusões, é onde são identificadas todas as deficiências encontradas na análise do trabalho, assim como sugestões de oportunidades de melhoria correspondentes. Todas as deficiências quer no D&I como na operacionalidade têm de estar identificadas, de forma que o cliente identifique o problema e o possa corrigir após a auditoria.

Associado a cada deficiência, existe um risco compreendido numa escala de 1 a 3. A escala do risco encontra-se descrita na secção 2.2.5.

No final, apenas o Memo de Conclusões é enviado para o cliente de modo a este ter conhecimento de todas as deficiências identificadas na análise ao sistema em causa, servindo como guia de melhorias a serem implementadas na empresa, com o intuito de mitigar os riscos associados a cada Objetivo de controlo.

Fase IV

Esta fase apenas se aplica, a clientes que em anos anteriores tenham sido auditados pela equipa de ERS. O objetivo é realizar um mapeamento entre os níveis de riscos que foram detetados no ano anterior e os que foram detetados no ano corrente. Este exercício é realizado para demostrar ao cliente a evolução que obteve de um ano para o outro e a quantidade de riscos que foram mitigados.

3.3. Ferramentas e Tecnologias

Nesta secção encontram-se descritas as ferramentas, nomeadamente: *Audit Command Language* (ACL), Audit System 2 (AS/2), que foram utilizadas para a realização do estágio.

3.3.1. *Audit Command Language* (ACL)

O *Audit Command Language* (ACL) é uma ferramenta utilizada pela Deloitte para fazer auditorias à qualidade da execução das atividades de controlo.

O ACL é uma aplicação de *software* para a execução de ficheiros interrogatórios [6]. Os ficheiros interrogatórios são usados em processos que nos permitem automatizar alguns testes de auditoria, conseguindo-se obter um acesso rápido e flexível a várias entidades de dados. Este processo também pode ser chamado de "Exploratory data analysis" (EDA). Um exemplo de um ficheiro interrogatório, pode ser uma tabela .csv, e.g., com 1 milhão de registos. Os tipos de ficheiros mais utilizados encontram-se separados por tab ou virgulas, tal como exemplifica a seguinte [6]:

NR_PROD	DESC_PROD	QUANT	CUSTO_UN	CUSTO_TOT
281705	Tubos	456	124.75	56886
281706	Chave Fendas	1235	38.94	48090.9
281707	Martelos	88	513.44	45182.72
281708a	Serrotes	56	1237.26	69286.56

"*Delimited Text Files*":

```
NR_PROD|DESC_PROD|QUANT|CUSTO_UN|CUSTO_TOT
281705|Tubos|456|124.75|56886
281706|Chave Fendas|1235|38.94|48090.9
281707|Martelos|88|513.44|45182.72
281708a|Serrotes|56|1237.26|69286.56
```

"*Fixed Record*":

```
NR_PRODDESC_PROD    QUANTCUSTO_UNCUSTO_TOT
281705 Tubos        456  124.75   56886
281706 Chave Fendas1235 38.94    48090.9
281707 Martelos     88   513.44   45182.72
281708aSerrotes     56   1237.26  69286.56
```

Imagem 14 - Importação de Ficheiros interrogatórios

O ACL auxilia na análise dos arquivos, aumentando a compreensão de uma grande quantidade de registos (não contendo limite de registos), sendo possível realizar análises sobre esses registos, o que manualmente (e.g. com a utilização o Microsoft Excel), seria impossível de realizar (e.g. vários registos com muitas transações para testar como é o caso do sector bancário).

Porquê a utilização do ACL?

Como já foi referido anteriormente trata-se de uma ferramenta para a realização de auditorias e gestão de risco. Permite realizar controlos internos de forma a identificar a mitigação dos riscos, proteger lucros e acelerar o desempenho. A Deloitte, com a utilização do ACL, garante ao cliente que a informação em análise não é corrompida, ou seja, os dados fonte fornecidos pelos clientes terão sempre uma segurança de não adulteração durante a sua análise. Toda a família Deloitte utiliza o ACL para realizar as análises aos dados, de forma a efetuar a sua validação. Assim sempre que é necessário passar informação entre departamentos, todos se encontram familiarizados com a ferramenta.

Vantagens do ACL

O ACL é uma ferramenta que se assemelha muito com o *software* Microsoft Excel, sendo este familiar para a maioria das empresas. No entanto, o ACL tem vantagens em relação ao *Microsoft Excel, que* são as seguintes:

- O ACL protege a integridade dos seus dados de origem;
- Possibilidade de trabalhar com uma grande quantidade de registos, sendo o número de registos limitados consoante o tamanho do disco rígido. O *Microsoft Excel* tem um limite máximo de 65.536 linhas;
- O ACL adapta-se a uma ampla quantidade de tipos de dados e tipos de arquivos. O ACL consegue ler ficheiros do tipo ASCII (como o Excel), e também arquivos do tipo EBDIC de *mainframe computers* no seu formato original que são interpretados pelo ACL sem necessidade de reformatar/traduzir os dados. O ACL importa dados, através da leitura de campos numéricos com cifrões, *brackets* e virgulas, mesmo que os sinais se encontrem à esquerda ou à direita;

- O *layout* das tabelas também pode ser definido no ACL, e.g., se o utilizador tiver várias tabelas iguais, pode aplicar a formatação apenas à primeira, que depois basta replicar essas mesmas formações para as restantes, sendo que a eliminação e inserção de colunas também entra para esta formatação;
- O ACL também possibilita a visualização das tabelas em várias perspetivas, mantendo sempre os dados subjacentes. Uma tabela pode ter mais do que uma perspetiva, que permite reformatar as vistas individualmente, possibilitando ao utilizador a realização de diversas análises relativamente a cada tabela;
- A análise de apenas uma parte dos dados também é possível em ACL, sem a necessidade de os remover da tabela. Facilmente se ocultam com o auxílio de exceções, sendo depois possível analisar os restantes;
- Com o ACL é possível utilizar campos sobrepostos (e.g. selecionar os funcionários de uma empresa cujo o seu número de trabalhador inicie por 50). No Excel, seria necessário realizar uma coluna auxiliar para realização do filtro ou utilizar fórmulas mais complexas.
- O ACL possui um registo de todas as atividades que são realizadas pelo utilizador. O ACL possui de uma *tab*, onde o utilizador pode ver/ rever todas as suas atividades por ordem cronológica e guardá-las por completo ou apenas uma parte do log para arquivo. Ajuda muitas vezes os auditores a documentar o trabalho. Quando o Log é exportado, este vem num formato Excel AS/ 2 (ferramenta de documentação de auditorias da Deloitte).
- Terminologia:
    - "Registo": equivalente a uma linha do Excel; e
    - "Campo": equivalente a uma coluna no Excel.

O ACL consegue ler vários tipos de ficheiros, entre os quais:

- Access;
- dBase (.dbf);
- DelimitedText Files (.csv);
- Excel;
- PDFs;
- XML;e
- *Fixed Record.*

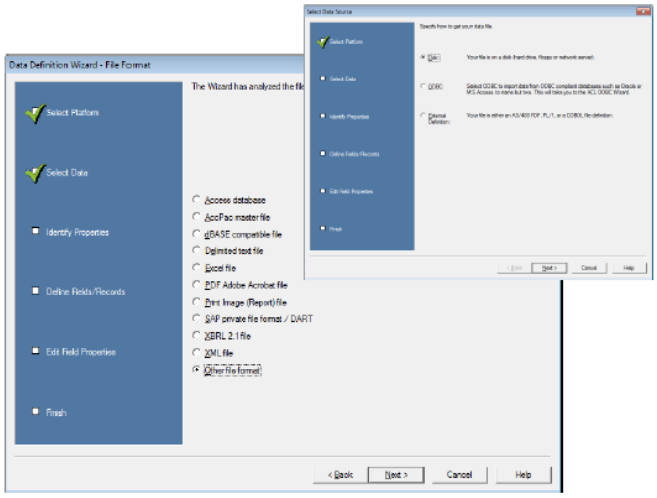

Imagem 15 - Importação de dados ACL

Não aceita:

- Programas executáveis ("*.exe*", "*.com*");
- *Backups*; e

- *Mainframe data bases.*

O ACL implica a disponibilidade de recursos em **disco rígido de 2,5x o tamanho do ficheiro** de dados, sendo que estes podem estar dispersos por várias tabelas, cada tabela correspondendo a um ficheiro .FIL. A partir do ACL é possível extrair tabelas com determinados registos ou campos não sendo necessário extrair a totalidade dos campos ou registos [7]. A seguinte Imagem 16 exemplifica como é a estrutura de dados do ACL:

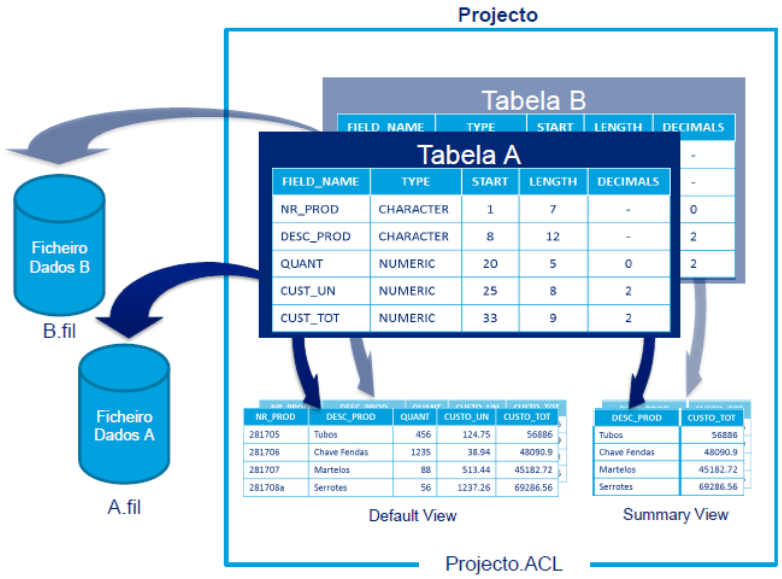

Imagem 16 - Estrutura de dados ACL

Comandos ACL

Tabela 5 - Comandos ACL

Comando	Descrição e Comando
Extract	Cópia de determinados registos ou campos do ficheiro corrente (nota: não tem que ser necessariamente a totalidade dos campos ou registos). `EXTRACT FIELDS <nome_campos> TO <tab_destino><IF condição><APPEND>`
Export	Exportar o ficheiro para outras aplicações, (e.g. para o excel, dbase,word) para futuras análises. `EXPORT FIELDS <nome_campos> TO <fich_destino><tipo_ficheiro>`
Classify	Conta registos relacionados com um único campo (ASCII) e acumula os resultados em um ou vários campos numéricos. `CLASSIFY ON <nome_campo> SUBTOTAL <nome_campos> TO <destino>`
Summarize	Agrupa por uma ou mais variáveis os totais dos campos numéricos seleccionados e conta quantos registos existem de cada um dos valores dessas variáveis. `SUMMARIZE ON <nome_campos> SUBTOTAL <nome_campos><OTHERoutros_campos> TO <destino><PRESORT>`

Gaps	Análise da sequência de um determinado campo, identificando registos de numeração em falta. `GAPS ON <campos_numéricos> TO <destino><PRESORT>`
Duplicates	Análise da sequência de um determinado registo, identificando se estes têm duplicados. `DUPLICATES ON <nome_campos> OTHER <nome_campos> TO <destino><PRESORT>`
Sort	Ordenar o ficheiro corrente numa ordem ascendente ou descendente considerando para o efeito o campo chave específico. O resultado da actividade de ordenação é guardado num novo ficheiro. `SORT ON <nome_campos> TO <destino>`
Age	Cálculo da antiguidade, face a uma data de referência, acumulando por intervalo de dias o despectivo valor. `AGE ON <campo_data><CUTOFFyyyymmdd><INTERVAL intervalos><SUBTOTAL campos_numéricos> TO <destino>`
Verify	Verificar a existência de erros no ficheiro, pela comparação dos diversos campos e o que foi definido no formato de cada campo (no Table Layout) `VERIFY FIELDS <nome_campos> TO <destino | PRINT>`
Statistics	Realizar estatísticas descritivas campos numéricos ou campo data num ficheiro corrente de dados `STATISTICS <campo_numérico><STD><NUMBER n> TO <destino | PRINT>`
Join	Junta campos de dois ficheiros de entrada ordenados num terceiro. `JOIN <tipo_de_join> PKEY <chave_tab_prim> FIELDS <campos_tab_prim> SKEY <chave_tab_sec><WITH campos_tab_sec><IF condicao> TO <destino><PRESORT><SECSORT>` Tipos de Join: • `PRIMARY:` Mantem todos os registos da tabela primária; • `SECONDARY:` Mantem todos os registos da tabela secundária; • `PRIMARY SECONDARY`: Mantem todos os registos de ambas as tabelas; • `UNMATCH:` Mantem os registos da tabela primária que não existem na tabela secundária; e • `MANY:` Combina todos os registos da tabela primária com toda a informação da tabela secundária.

De seguida pode-se observar um pequeno excerto de código realizado no ACL, para o leitor ter uma visão mais detalhada do que foi descrito anteriormente. Este exemplo trata de dados de uma urgência, tendo como objetivo monitorizar o tempo médio de espera dos utentes. Pode ser observado através da Imagem 17 que se segue:

```
Comment filtra apenas as urgencias nos seis primeiros meses
OPEN Tabela_Urgencias
GROUP
Mes = SUBSTR(DT_ENT_URG,4, 2)
EXTRACT FIELDS ALL mes IF ( BETWEEN(SUBSTR(DT_ENT_URG,4, 5), "01", "06") AND NOT MATCH(FLG_ESTADO,"A") ) TO
"Tabela_Urgencias_Aux"
END

Comment Apura o numero de utentes atendidos na urgencia por mes, SUMMARIZE agrupa por mes e conta (Denominador)
OPEN Tabela_Urgencias_Aux
SUMMARIZE ON Mes TO "Tabela_urgencia_summarize" PRESORT

comment junção MANY das tabelas anteriormente trabalhadas, com ordenação em ambas as tabelas
OPEN Tabela_Urgencias_Aux
SORT ON DOENTE TO Tabela_pri
SORT ON DOENTE TO Tabela_sec
OPEN Tabela_pri PRIMARY
OPEN Tabela_sec SECONDARY
JOIN MANY PKEY DOENTE FIELDS DOENTE EPISODIO AS "EPISODIO1" DT_SAIDA_URG HR_ALTA SKEY DOENTE WITH DOENTE EPISODIO AS
"EPISODIO2" DT_ENT_URG HR_ENT TO Tabela_Join OPEN PRESORT SECSORT
CLOSE SECONDARY

comment calculo/filtro da diferença entre as duas datas e filtro de episodios iguais
OPEN Tabela_Join
GROUP
MES = SUBSTR(DT_ENT_URG,4, 2)
data_alterada= AGE(CTOD(DT_SAIDA_URG, "DD-MM-YYYY"),CTOD(DT_ENT_URG, "DD-MM-YYYY"))
EXTRACT FIELDS ALL MES IF (EPISODIO1<>EPISODIO2) AND MATCH(data_alterada,1,0) TO Tabela_data
END
```

Imagem 17 - Exemplo de código ACL

Testar a ordem sequencial – Ordenação e Indexação

O ACL tem a possibilidade de verificar se os dados já se encontram numa ordem sequencial, ou seja, se a tabela já foi ordenada ou indexada. Esta opção, possibilita também ao utilizador identificar itens fora da sequência de dados, que têm uma ordem sequencial inerente, como por exemplo uma fatura com possíveis irregularidades.

Dois métodos de ordenação são a ordenação e a indexação que realizam uma ordenação sequencial dos dados nas tabelas. Sendo que, o ACL processa os arquivos de forma sequencial, ordenar os dados em sequência é um pré-requisito para alguns testes analíticos, como para operações realizadas no ACL. Pode dar-se também a situação de testes e operações do ACL serem realizadas mais rapidamente, tendo os dados sido primeiramente ordenados ou indexados. Um exemplo destas operações, podem ser associações e relações, tendo estas como pré-requisito uma ordenação ou uma indexação dos pares chave-valor. [7]

Como já foi referido, os testes de ordem sequencial são realizados sequencialmente. O utilizador é informado se um par de valores constitui uma quebra na sequência, sendo que, depois desta quebra, a sequência é reiniciada usando o segundo dos valores em pares como um novo ponto inicial. Todos os valores seguintes à quebra que estejam fora da sequência, ao serem comparados com valores anteriores à quebra, não são reportados como erros de sequência. Vejamos o seguinte exemplo: vamos testar os seguintes valores da coluna em ordem crescente, o ACL informa dois erros de sequência (4;1), mas não cinco (4; 4; 5; 1; 2). A tabela 1 exemplifica o teste, que foi referido:

Tabela 6 - Exemplo teste em ordem sequencial

1	
3	
6	
4	Erro de sequência
4	
5	
6	
9	
1	Erro de sequência
2	

Indexação

A indexação em ACL, quando é realizada, resulta na criação de um arquivo separado, com a extensão **.inx**, que permite o acesso aos registos numa tabela do ACL através de uma ordem sequencial, em vez de ir a uma tabela já ordenada previamente. De notar que os índices não reordenam os dados fisicamente em tabelas, no entanto, quando temos uma tabela com o índice ativo, os dados que estão a ser trabalhados são reorganizados com a ordem especificada pelo índice e operações analíticas processam os dados baseados nessa ordem. Quando deixam de estar ativos, os registos em exibição são revertidos para a forma original (física). Os índices podem ser aplicados a qualquer tipo de campos, incluindo campos calculados e expressões *ad hoc*, independentemente do tipo de dados que estejamos a tratar.

Através do ACL é possível criar vários índices para uma única tabela, podendo também trocá-los caso necessário, esta operação pode ser útil para avaliar inicialmente um conjunto de dados. Apenas um índice pode ser ativado de cada vez. Se uma tabela tiver mais que uma exibição, todas estarão sujeitas a um índice ativo.

O ACL permite indexar a partir de um chave-valor ou criar esquemas de indexação, ou seja, indexar vários campos chave-valor (chave-valor primário, chave-valor secundário, etc.). É possível misturar a indexação uma por ordem crescente e outra por ordem decrescente, misturando os tipos de dados em campos chave-valor. A Tabela 7, realiza indexação por ordem crescente num campo de dados e, em cada dia, por ordem decrescente num campo chave-valor:

Tabela 7 – Exemplo indexação

15 Janeiro de 2015	2.000 €
15 Janeiro de 2015	1.200 €
15 Janeiro de 2015	600 €
16 Janeiro de 2015	900 €
16 Janeiro de 2015	100 €
17 Janeiro de 2015	4.700 €
17 Janeiro de 2015	900 €
17 Janeiro de 2015	500 €

Ordenação vs Indexação

O ACL ordena os dados sequencialmente como já foi referido anteriormente. A ordenação de uma tabela física é realizada da seguinte maneira: o ACL reordena os dados em ordem sequencial e guarda-os numa nova tabela **.FIL**, ao contrário da indexação que não altera a ordem física dos dados.

Antes de se realizar qualquer uma das operações é necessário ver qual a que se adequa mais ao trabalho que se quer realizar. Por exemplo, a ordenação pode ser mais vantajosa para um trabalho de investigação, por criar uma nova tabela onde esta pode ser usada futuramente. A indexação pode ser mais vantajosa para trabalhos informacionais ou preliminares.

Ordenar uma tabela é mais lento e requer mais espaço em disco do que a indexação, mas torna-se mais rápido realizar análises subsequentes numa tabela ordenada do que numa tabela indexada, ou seja, se estamos perante uma grande quantidade de dados, pode ser mais vantajoso ordenar a tabela para otimizar a velocidade de processamento subsequente. Mas se o espaço de disco é limitado e o utilizador precisar de uma ordenação mais rápida o ideal é indexar.

3.3.2. Audit System 2 (AS/2)

O *software Audit System* 2, é uma ferramenta criada e utilizada pela Deloitte. Esta ferramenta possibilita o armazenamento de todas as Auditorias realizadas pela Empresa. Todos os documentos realizados no âmbito de uma auditoria, bem como todas as evidências fornecidas pelos clientes, devem ficar armazenados num ficheiro AS/2.

Cada ficheiro AS/2 corresponde a um projeto, sendo este preenchido ao longo de toda a auditoria. Uma das grandes vantagens que o AS/2 proporciona, é a possibilidade de extração de um ficheiro, contendo toda a informação. Assim este ficheiro pode ser enviado e importado em qualquer máquina que contenha o *software*, com a maior das facilidades. Mesmo quando é necessário transferir ou atualizar apenas alguns ficheiros que estejam dentro do ficheiro do projeto, é possível realizar um *transfer*. Mais uma vez é importado com todas as facilidades e adiciona ou atualiza os ficheiros do projeto.

AS/ 2 - CGI

O ficheiro da ferramenta AS/2 a utilizar numa CGI deverá ser o mesmo utilizado pela equipa de auditoria financeira — esta deverá fornecer o respetivo pack AS/2 (antes do início do projeto). O ficheiro deve conter a seguinte informação:

- Toda a documentação digital recebida do cliente (evidências) que deverá ser anexada à pasta AS/2 do projeto em questão, sendo cada uma devidamente numerada;
- Sempre que possível, a documentação recebida em papel deverá ser digitalizada e anexada na pasta AS/2;
- Do mesmo modo, a documentação em papel deverá ser referenciada na pasta AS/2 do projeto em questão (e arquivada na pasta física respetiva).

A Imagem 18 seguinte ilustra um exemplo de um projeto AS/2.

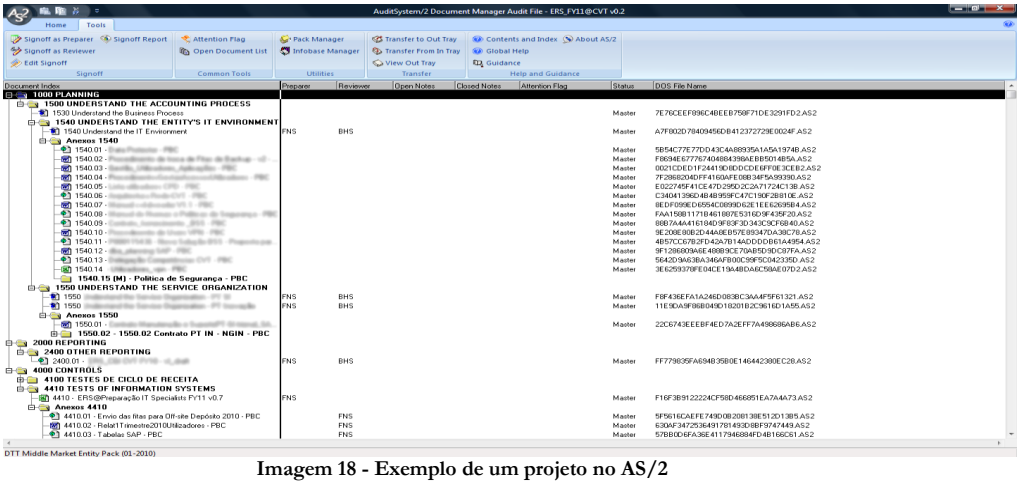

Imagem 18 - Exemplo de um projeto no AS/2

No final do projeto deverá existir uma pasta física deste, onde deverão ser arquivados todos os documentos em papel facultados pelo cliente e relevantes para projeto em análise. Todos os documentos recebidos ou produzidos têm de ser assinados. Uma assinatura no AS/2 é uma assinatura digital, que permite identificar quem é que produziu/ reviu a CGI. A assinatura é composta pelas primeiras letras do nome (e.g. MSM – Mariana Sofia Moutinho) de quem executa e revê a CGI, sendo que existem dois tipos de assinaturas:

- "Preparer": são assinaturas de quem realiza o documento de controlo. Deve ser assinado por *Analysts*, *Consultants* e *Senior Consultants*; e
- "Reviewer": são assinaturas de quem revê o documento de controlo. Deve ser assinado por um *Manager* ou por um *Partner*.

Apenas os documentos facultados pelos clientes são assinados pelos *Analysts, Consultants* ou *SeniorConsultants* como "Reviewer".

A data das assinaturas deverá ser coerente com a data do relatório final de conclusões.

4. Auditoria a controlos informáticos

A operadora constatou que continuava a existir a necessidade de avaliação e controlo de riscos de segurança de informação dentro da sua organização, relativamente aos números pré-pagos e pós-pagos sobre a rede GSM.

Esta necessidade já tinha sido identificada na última intervenção da Deloitte nesta operadora, aquando da conclusão dos testes periódicos aos consumos e carregamentos dos números pré-pagos sobre a rede GSM.

4.1. Objetivos

Os objetivos do trabalho realizado na operadora incluíram o levantamento/entendimento dos processos de negócio com impacto na receita e a avaliação dos controlos aos SI/TI dos processos de consumos, carregamentos e faturação dos números pré-pagos e pós-pagos da rede GSM. Em seguida foi fundamental identificar os riscos associados à receita da operadora, com maior foco nos riscos de SI/TI, assim como definir os objetivos de controlo e as suas respetivas atividades de controlo.

Numa fase posterior foi necessário verificar a existência ou não de procedimentos documentados e aprovados pela gestão de topo; se os SI/TI estão adequados às necessidades da operadora; se o acesso à informação dos SI/TI estava restrito exclusivamente a pessoas devidamente autorizadas pela mesma operadora; se a informação dos SI/TI processos de consumos, carregamentos e faturação se encontrava devidamente atualizada e disponível; e ainda se existiam controlos internos relativos ao processamento da informação dos SI/TI, bem como se o seu registo era devidamente monitorizado.

Numa última fase, fez-se a análise dos resultados e emitiram-se as respetivas conclusões desta auditoria. Essas conclusões geraram a identificação de oportunidades de melhoria aos controlos de SI/TI dos processos de consumos, carregamentos e faturação dos números pré-pagos e pós-pagos da rede GSM.

4.2. Metodologia

A Imagem 19 representa o modelo PDCA utilizado neste trabalho e tem por base as normas 27001 e 22301 já referenciadas nas secções 3.1.2 e 3.1.3, do presente relatório.

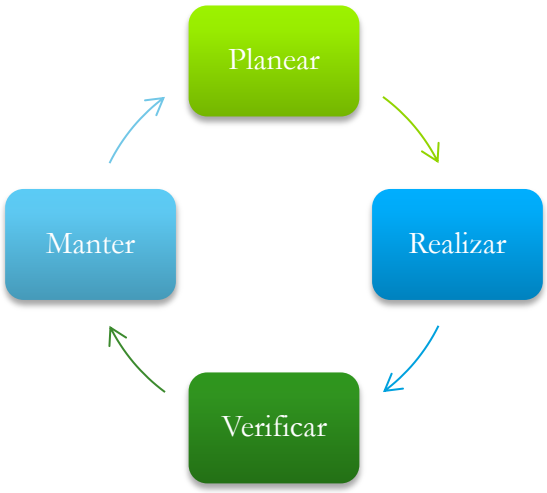

Imagem 19 - Metodologia do projeto

Este modelo PDCA apresenta quatro fases:

Planear

Nesta fase do projeto começou-se por definir os objetivos a alcançar e adquirir conhecimento sobre as características, a organização e os processos de negócio da operadora, bem como, as áreas de negócio com impacto na receita. Complementarmente, identificaram-se os riscos com impacto na receita, os *inputs* e *outputs* necessários para a realização do trabalho, os interlocutores intervenientes nos processos em estudo e definiram-se os riscos do projeto.

Realizar

Foram realizadas reuniões onde se fez o levantamento dos processos de negócio com impacto na receita. Documentaram-se os processos de negócio anteriormente levantados e identificaram-se os riscos. De seguida foram definidos os objetivos e atividades de controlo, de forma a mitigar os riscos.

Verificar

Esta fase iniciou-se com o desenho dos testes e procedimentos de avaliação, execução dos respetivos testes e emissão de conclusões.

Manter:

Nesta ultima fase, identificaram-se falhas nos processos com impacto na receita e indicaram-se as oportunidades de melhoria a implementar na operadora.

4.3. Abordagem

Na Imagem 20, pode-se observar as fases do projeto, que foi iniciado com um levantamento da realidade da operadora, seguindo-se a identificação dos riscos, dos objetivos e atividades de controlo, a execução dos testes dos controlos de SI/TI, a análise dos resultados e conclusões, finalizando com a apresentação de recomendações.
A fase "Gestão do projeto" engloba todas as outras fases, pois é necessário um acompanhamento continuo ao longo do trabalho. Adicionalmente, esta fase representa os pontos que serão apresentados de seguida, nomeadamente: equipa; abordagem e calendário.

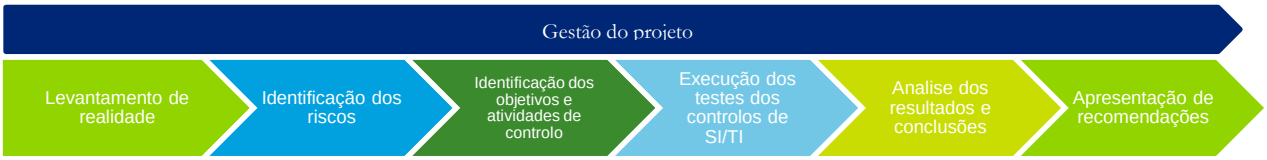

Imagem 20 - Fases do projeto

4.4. Equipa

O trabalho desenvolvido neste estágio foi enquadrado numa equipa composta por um *partner*, um *senior manager*, uma *senior consultant*, um *consultant* e dois *analysts*. A equipa é liderada pelo *partner,* que planeia o trabalho, o *senior manager*, que organiza o trabalho planeado e o faculta à *senior consultant*, que organiza e distribui o trabalho pelos diferentes elementos de acordo com experiência de cada um. Posteriormente, o *senior manager* recebe de volta o trabalho, valida e apresenta o trabalho ao *partner*, que exerce a validação final e apresenta o trabalho ao cliente. Com todo este processo a Deloitte consegue garantir um trabalho bem estruturado com uma qualidade de excelência.

O trabalho contém várias fases, sendo que cabe ao *senior manager* organizar e priorizar o trabalho. Muitas vezes esta priorização faz-se em conjunto com o cliente, de modo a que ambos os lados estejam em sintonia. Depois de todo o planeamento efetuado, como já foi referido anteriormente, este é distribuído consoante a experiência de cada membro da equipa. A validação do trabalho é realizada de baixo para cima, como se pode observar na Imagem 21, ou seja, o trabalho realizado pelos *analysts* é validado pelo *consultant* e assim sucessivamente.

Imagem 21 - Organização hierárquica da Deloitte

Na Imagem 22, que é apresentada a seguir, pode-se observar todo o processo do trabalho desenvolvido pela Deloitte, desde o seu planeamento até à apresentação do mesmo ao cliente:

Imagem 22 - Fluxo de trabalho Deloitte

4.5. Abordagem e calendário

O projeto foi iniciado com um período de formação aos novos elementos da equipa (analistas). Esta formação iniciou-se com uma "passagem de pasta" sobre a operadora, bem como o trabalho realizado pela equipa da Deloitte na sua última estadia na operadora. Uma "passagem de pasta" consiste no estudo do material disponibilizado pela equipa, ações de formação para esclarecimento de dúvidas e em alguns casos, realização de exercícios. No que respeita ao projeto, foram-nos fornecidos manuais explicativos do trabalho, onde tivemos a oportunidade de conhecer/ compreender o trabalho já realizado. Um ponto importante nesta "passagem de pasta" foi o entendimento dos testes periódicos, aos consumos e carregamentos dos números pós-pagos da rede GSM da operadora, de forma a detetar perdas na receita. Adicionalmente, existiram ações de formação, onde tivemos esclarecimentos sobre as metodologias da Deloitte, bem como das ferramentas necessárias para a realização do trabalho.

Sendo a finalidade do trabalho garantir a correta captação da receita, houve a necessidade de realizar um levantamento dos processos de negócio associados à receita da empresa. Foram efetuadas várias reuniões juntamente com os responsáveis dos departamentos que interagem diretamente com a receita da empresa. Após o entendimento dos processos de negócios foi necessário documentá-los identificando os riscos associados à receita da empresa.

Paralelamente, foram realizados testes periódicos aos consumos e carregamentos dos números pré-pagos GSM. Adicionalmente, foram ainda realizadas ações de formação com elementos da equipa do departamento de Receita e faturação da operadora, de forma a realizar também uma "passagem de pasta" dos testes periódicos dos consumos e carregamentos. Estes testes passaram a ser uma atividade de controlo realizada mensalmente pelos elementos do departamento de Receita e Faturação da operadora.

Estando os riscos identificados, foi decidido que existia a necessidade de realizar uma avaliação aos controlos dos sistemas de informação do processo de faturação da operadora. Iniciamos assim a segunda fase do trabalho na operadora. Como já tínhamos conhecimentos sólidos relativamente aos processos da empresa, foi apenas necessário efetuar reuniões juntamente com elementos da direção de sistemas de informação (DSI) da operadora para realizar o entendimento do processo de faturação relativamente aos sistemas de informação em âmbito (*Billing* GSM, Cobranças e Contabilidade). Após o entendimento finalizado, este foi devidamente documentado e estudado de maneira a identificar os riscos associados e respetivos objetivos e atividades de controlo. Aquando da identificação das atividades de controlo foram desenhados os testes a realizar aos três sistemas em âmbito, bem como os pedidos de informação necessário à realização dos mesmos.

Por último, foi realizado um relatório de conclusões das carências detetadas no trabalho e respetivas oportunidades de melhoria, tendo em vista ajudar a operadora a melhorar os controlos associados à receita da empresa.

Identificação dos riscos do projeto

Os riscos do projeto incluem os processos de planeamento, identificação, análise, planeamento de respostas, monitorização e controlo dos riscos do projeto. Os objetivos da gestão dos riscos são aumentar a probabilidade e o impacto dos eventos positivos e reduzir a probabilidade e o impacto dos eventos negativos no projeto.

A identificação dos riscos do projeto foi realizada sob a forma de um processo interativo de modo a chegar a um estado estável. Iniciou-se com uma explicação do nosso *senior manager* relativamente ao que era pedido. Depois dos riscos entendidos e detetados, foi realizada uma proposta. Posteriormente, esta proposta foi discutida em conjunto com a toda a equipa e foi alterada de acordo com as conclusões encontradas, até se chegar a um estado estável. O seguinte esquema clarifica este processo:

Imagem 23 - Elaboração dos riscos do projeto

Após a identificação dos riscos do projeto, foram tomadas medidas para os mitigar. Foram identificadas formas de mitigação do risco dependentes da Deloitte e outras dependentes da operadora. Se ambos os intervenientes seguirem as indicações descritas este tipo de risco fica com uma probabilidade reduzida de ocorrer, caso contrário o projeto pode ficar comprometido.

No **anexo 1**, encontram-se todos os riscos do projeto identificados, bem como as responsabilidades dependentes, tanto da Deloitte como da operadora.

Calendário

Imagem 24 – Planeamento trabalho

4.6. Levantamento da realidade

Nesta secção encontram-se descritos os procedimentos realizados para efetuar o trabalho na operadora. Estes procedimentos passam por um levantamento dos processos de negócio, que até à data a operadora não possuía, entendimentos dos sistemas a avaliar e por fim, a organização dos processos e suporte dos sistemas em âmbito.

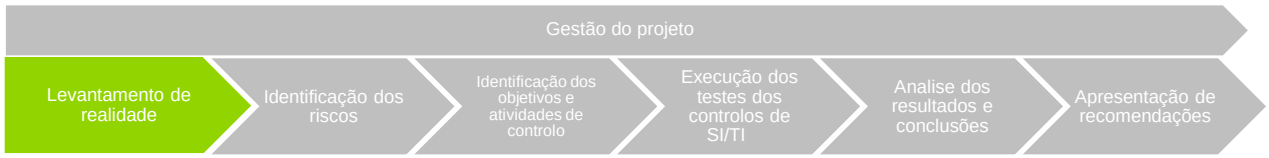

Imagem 25 - Fase levantamento da realidade

4.6.1. Processos e objetivos de negócio

Um processo de negócio é constituído por um número de atividades que têm se ser executadas, reguladas por um conjunto de condições que determinam a ordem das atividades, com o objetivo de produzir um serviço, que tem valor específico para o cliente. Uma atividade é uma unidade lógica de trabalho que é executada como um elemento ligado a um recurso. Um recurso é um nome genérico para uma pessoa, máquina ou um grupo de pessoas ou máquinas que realizam tarefas específicas. [8]

O sucesso de qualquer organização depende de uma correta definição dos processos de negócio. Para isso, é necessário identificar e planear os seguintes pontos:

- Missão da empresa;
- Visão da empresa;
- Valores da empresa;
- Entidades:
    - Fornecedores;
    - Clientes;
    - Colaboradores da empresa;
    - Produtos; e
    - Serviços.
- Quais os departamentos da empresa, bem como, quais as suas funções e responsabilidades; e
- Que atividades são necessárias serem executadas.

Objetivos do levantamento dos processos de negócio

Na operadora em estudo, a finalidade para o levantamento dos processos de negócio, são os seguintes:

- Conhecimento do negócio da empresa mais pormenorizado;
- Conhecimento dos processos de negócio com impacto para a receita da empresa;
- Conhecimento das atividades, bem como todas as suas características, nomeadamente:
    - Prioridade;
    - Procedimentos;
    - Sistemas;
    - Intervenientes; e
    - Departamentos que interagem com cada atividade.
- Conhecimento de todos os departamentos/ intervenientes que interagem com o controlo da receita;
- Deteção de problemas que podem afetar o trabalho de cada colaborador da empresa, de modo a evitar inconvenientes, nomeadamente:

    - Repetição de tarefas;
    - Dependência de trabalho de terceiros;
    - Desmotivação; e
    - Queda de produtividade.
- Identificação de soluções para reduzir as carências identificadas anteriormente.

Fases do levantamento dos processos de negócio

O levantamento dos processos de negócio passou por várias fases, até à sua documentação, nomeadamente:

- Identificação dos departamentos com impacto na receita;
- Comunicação aos departamentos do valor que o trabalho iria fornecer à empresa e agendar reuniões de esclarecimentos;
- Realização de reuniões com os responsáveis dos departamentos de forma a efetuar a compreensão dos processos com impacto na receita;
- Desenho de diagramas para documentar todas as atividades realizadas em cada processo, estando estas separadas por etapas e responsáveis. Como pode ser exemplificado através da Imagem 26;
- Realizações de reuniões com os responsáveis de cada departamento, com o objetivo destes procederem a uma validação dos fluxos anteriormente realizados;
- Proceder às correções dos fluxos, caso necessário; e
- Produção dos documentos denominados como "Entendimento de Processos", com a finalidade de documentar todos os fluxos, bem como o entendimento adquirido no levantamento dos processos de negócio.

Na Imagem 26, que se segue podemos observar todo o processo de levantamento de processos:

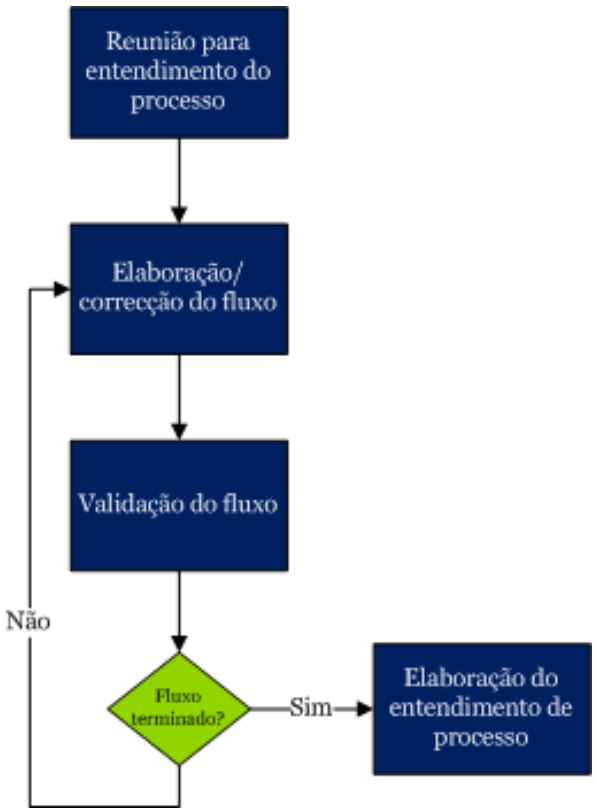

Imagem 26 - Fases do levantamento dos processos

Representação de processos de negócio

Apesar da existência de notações *standard* para a representação dos fluxos dos processos de negócio, como é o caso do BPMN [9] os processos do cliente não foram documentados com esta abordagem, porque o cliente já se encontrava familiarizado com o *template* da Deloitte, daí a decisão de permanecer com a mesma estrutura.

As atividades de cada fluxo são representadas na tabela que se segue:

Tabela 8 - Descrição atividades fluxos

Representação	Descrição	Exemplo
AX. Actividade de natureza automática <sistema>	Atividades automáticas são realizadas automaticamente pelo sistema de informação, sem a necessidade da interação do homem.	Atualização do estado dos cartões. Os cartões após a sua utilização são imediatamente inativados.
AX. Actividade de natureza semi-automática <sistema/ evidência>	Atividades semiautomáticas são realizadas com a interação do homem e de um sistema.	Criação de uma nota de crédito, no sistema de Contabilidade.

AX. Actividade de natureza manual <evidência>	Atividades manuais, são realizadas apenas a partir do homem, sem a necessidade de nenhum sistema associado.	Validação da análise dos dados relativamente às faturas.
AX. Actividade X (responsável externo)	Atividade externa à organização, ou seja, prestam serviços à empresa ou a empresa presta um serviço.	Carregamento de saldo por parte do cliente final.
PX. <nome do processo>	Quando é necessário referenciar que determinada atividade é encaminhada para outro processo.	Encaminhamento para o processo de vendas.

O fluxo encontra-se dividido em duas componentes, sendo estas as seguintes:

- **Etapa:** representa a fase em que o fluxo se encontra (e.g. a primeira fase do fluxo é receber a reclamação do cliente, a segunda será proceder à analise da mesma);
- **Responsável:** representação do departamento que está responsável por realizar a atividade.

No fluxo que se segue podemos observar um fluxo fictício, para exemplificar tudo o que foi descrito anteriormente:

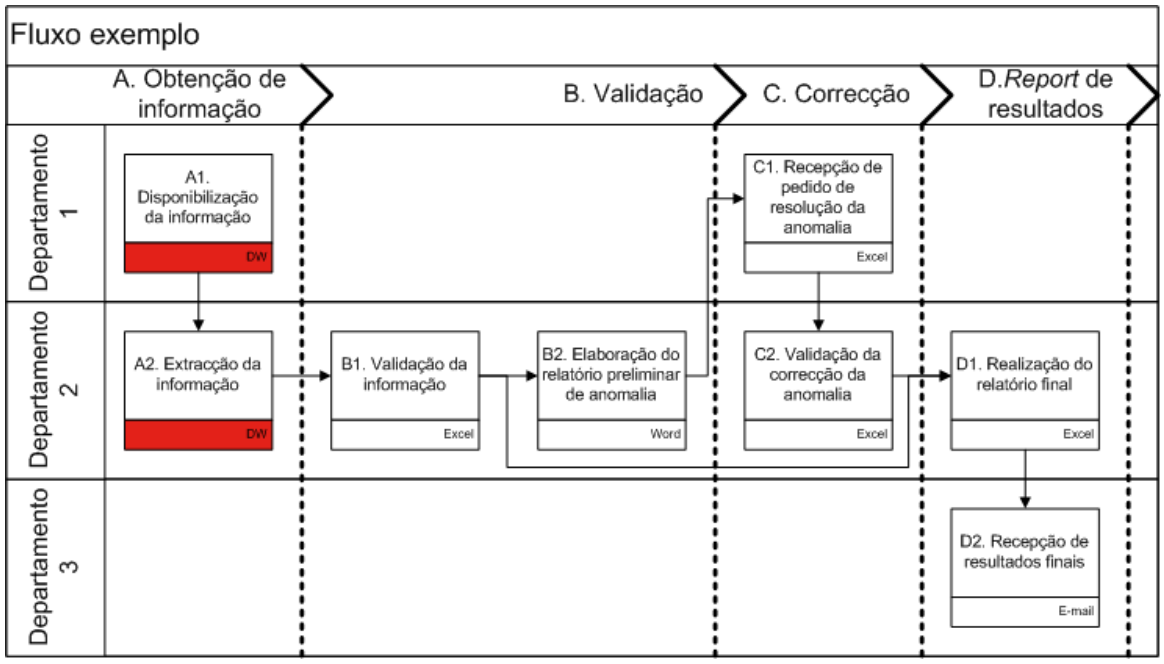

Imagem 27 – Fluxo exemplo

4.6.2. Sistemas e tecnologias de informação

O estudo dos sistemas de informação é um ponto fulcral na realização do trabalho, pois é nestes sistemas de informação, que vamos incidir o trabalho. Após o levantamento dos processos de negócio foi possível obter uma visão mais pormenorizada do funcionamento de cada sistema de informação.

Os sistemas de informação, que foram avaliados correspondem aos processos de Carregamentos e Consumos dos números pré-pagos da rede GSM e o processo de Faturação dos números pós-pagos da rede GSM.

De seguida apresenta-se os três sistemas de informação, que foram avaliados no âmbito deste trabalho, nomeadamente:

- **Sistema *Billing* GSM:** é o sistema responsável pela gestão de saldos e consumos para os números pré-pagos e pós-pagos da rede GSM. Este sistema é da total responsabilidade do parceiro de negócio da operadora (PNO);
- **Sistema Cobranças:** é o sistema de frente de loja, contém todas as funcionalidades de um sistema POS (*Pointof sale*). Onde os colaboradores da operadora podem consultar produtos, registar vendas e emitir faturas a clientes finais; e
- **Sistema Contabilidade:** é o sistema de contabilidade, sendo este o responsável pela integração dos seguintes componentes:
    - Venda de recargas;
    - Carregamentos; e
    - Consumos.

4.6.3. Fluxo de integração da informação

Carregamentos & Consumos

A integração da informação no processo de carregamentos e consumos dos números pré-pagos da rede GSM. A Imagem 28 apresentada de seguida, ilustra todo o fluxo de integração dos carregamentos e consumos, na contabilidade.

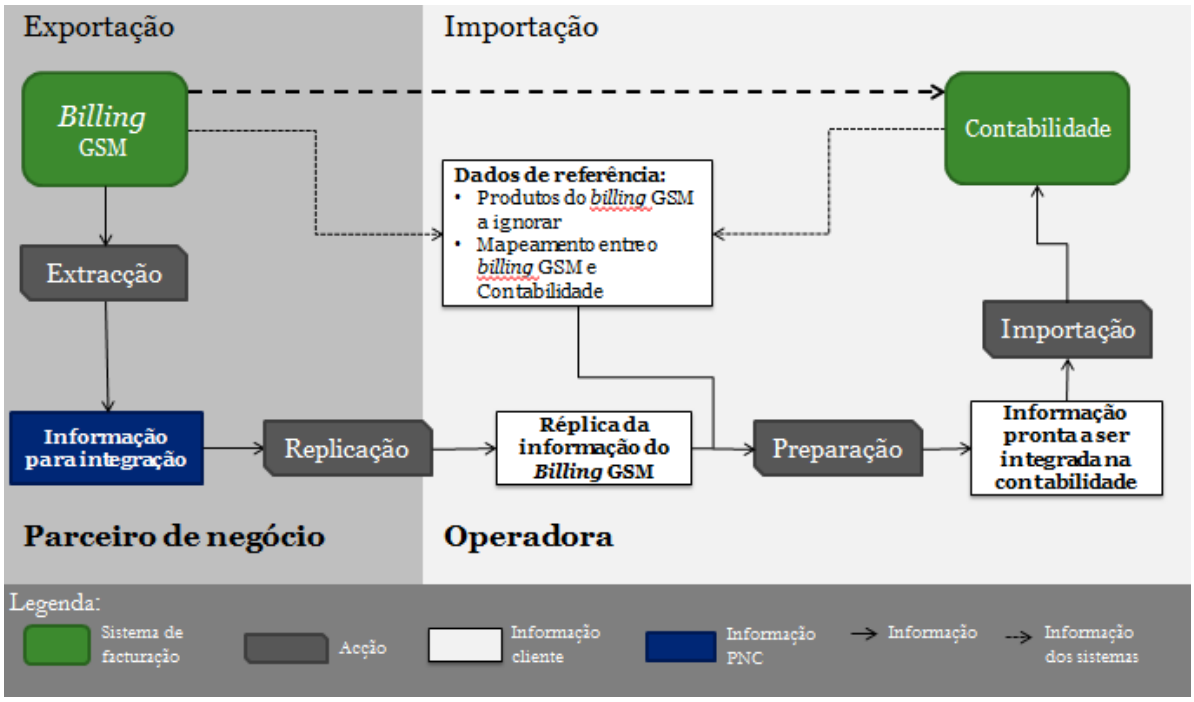

Imagem 28 - Integração na contabilidade

Entendimento:

A área cinza escura corresponde à extração da informação e é realizada por um parceiro de negócio da operadora (PNO), enquanto a área cinza clara corresponde à integração na contabilidade que é realizada pelo Departamento de Sistemas de Informação da operadora (DSI).

Ações:

- **Extração:** é a informação que é retirada do *billing* GSM de modo a ser integrada na contabilidade.
- **Replicação:** cópia realizada à informação de modo a pertencer à operadora;
- **Preparação:** a informação é filtrada (e.g. produtos a ignorar) e trabalhada de modo a ser integrada na contabilidade; e
- **Importação:** integração da informação na contabilidade.

O processo inicia-se quando o parceiro de negócio da operadora (PNO) extrai e disponibiliza a informação, que se encontra no sistema de *billing* GSM. A informação que é extraída corresponde aos carregamentos e aos consumos de saldo dos números GSM. Essa informação é disponibilizada numa base de dados SQL, à qual o DSI tem acesso, considerando o período de faturação do mês corrente, ou seja, do dia 25 do mês anterior ao dia 24 do mês corrente, inclusive (e.g. para o período correspondente ao mês se Dezembro,

a informação disponibilizada será relativamente ao período compreendido entre o dia 25 de Novembro e o dia 24 de Dezembro, inclusive).

A equipa do DSI, depois de receber toda a informação na base de dados, realiza uma cópia de toda a informação para uma base de dados local. Ainda nesta fase, são aplicadas regras de negócio à informação fornecida pelo PNO, através da utilização de dados de *billing* GSM e contabilidade, de forma a preparar a informação para ser integrada na contabilidade.

Faturação

Os consumos dos números pós-pagos GSM são geridos e registados no sistema de *billing* GSM e, mensalmente, consolidados na faturação GSM, que é integrada nos sistemas Cobranças e Contabilidade

A integração da faturação dos números pós-pagos da rede GSM, na contabilidade encontra-se apresentada na Imagem 29.

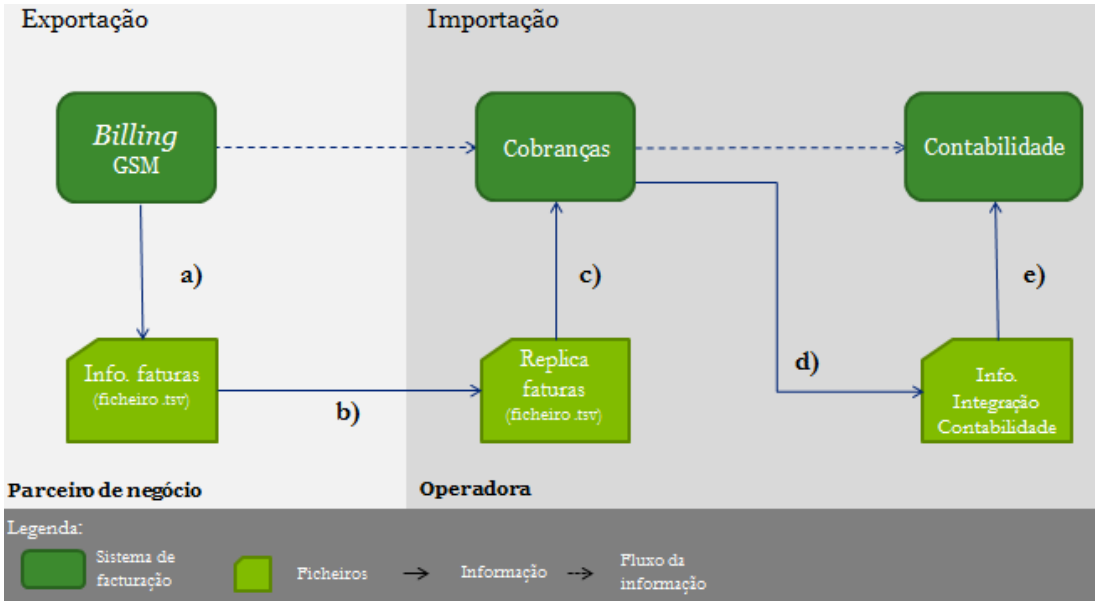

Imagem 29 - Fluxo de integração da faturação no sistema cobranças e contabilidade

Em cada período de faturação (inicio de cada mês), a faturação dos números pós-pagos GSM é gerada no sistema de *billing* GSM e integrada numa base de dados local, onde ficam registados os pagamentos efetuados pelos clientes. No final de cada mês, a informação da faturação dos números pós-pagos GSM, que se encontra na base de dados local, é integrada no sistema de contabilidade.

a) O parceiro de negócio da operadora, mensalmente realiza a faturação dos números pós-pagos GSM, de acordo com os consumos que foram registados, durante o período de faturação no sistema de *Billing* GSM. Quando este processo se encontra terminado é gerado um ficheiro (.tsv) com a informação das faturas dos números pós-pagos GSM;

b) A operadora recebe a informação gerada anteriormente e realiza uma cópia dos dados de modo a serem importados numa base de dados local;

c) A DSI é responsável por aplicar regras de negócio à informação que acabou de receber, através da utilização de alguns dados de referência, de forma a serem importadas as faturas, no sistema de Cobranças;

d) Mensalmente, a equipa da DSI é responsável por preparar a informação de faturação dos números pós-pagos GSM integrados no sistema de Cobranças, através da aplicação de regras de negócio e da utilização de informação de referência, para ser integrada no sistema de Contabilidade; e

e) Após a preparação da informação, a DSI é responsável por importar as faturas dos números pós-pagos GSM para o sistema de contabilidade onde é realizado o seu reflexo contabilístico.

4.6.4. Organização e processos de suporte SI/TI

Esta secção, tal como já se encontra explicado na secção 3.2.3 (Fase 1) do presente relatório, pretende-se descrever como está organizada à área de SI/ TI da operadora, assim como os principais processos de gestão e controlo dos SI/ TI, de forma a permitir obter um entendimento geral do ambiente de controlo implementado.
Neste contexto as principais áreas a analisar são:

- Gestão de operações;
- Segurança da informação; e
- Gestão de alterações.

Entendimento dos SI/TI e organização da DSI

O ambiente das aplicações em âmbito é caracterizado da seguinte forma:

Tabela 9 – Sistemas em âmbito

Sistemas	Sistema Operativo	Base de dados
***Billing* GSM**	Windows Server 2008	Microsoft SQL Server 2008
Cobranças	Windows Server 2008	Microsoft SQL Server 2008
Contabilidade	Windows Server 2008	Microsoft SQL Server 2008

Fornecedores externos

Parceiro de negócio da operadora

Todas as atividades relativas à administração do sistema Billing GSM e da sua manutenção (corretiva e evolutiva) são da responsabilidade do parceiro de negócio da operadora.

Existem dois contratos de prestação de serviços entre a operadora e o parceiro de negócio, nomeadamente:

- Suporte funcional: envolve manutenção evolutiva e corretiva; e
- Suporte técnico: envolve os serviços de disponibilização e manutenção de infraestrutura aplicacional de suporte e serviços de administração de sistemas.

Os contratos referenciados anteriormente, encontram-se em vigor e estão devidamente assinados por ambas as partes.

Fornecedor externo de apoio aos sistemas

Algumas atividades relativas à manutenção (corretiva e evolutiva) dos sistemas de Cobranças e Contabilidade são da responsabilidade do fornecedor externo de apoio aos sistemas.

Existe um contrato de prestação de serviços entre a operadora e o fornecedor externo. O contrato engloba suporte funcional (manutenção evolutiva e corretiva), estando em vigor e devidamente assinado por ambas as partes.

Informação do sistema organizacional e pessoal

Todas as atividades de gestão dos sistemas de Cobranças e Contabilidade, nomeadamente as relativas ao suporte são realizadas centralmente pelo departamento de sistema de informação da operadora (DSI), sendo esta gerida por um diretor.

No entanto, todas as atividades relativas ao sistema de informação *Billing* GSM, são realizadas por um parceiro de negócio, localizado em Luanda (e.g. gestão de operações, alterações, atribuição de acessos). O servidor do sistema *Billing* GSM encontra-se num CPD em Luanda.

As atividades de gestão e controlo de sistemas de informação estão centralizadas no DSI, que se encontra organizado da seguinte forma:

Tabela 10 - Organização do DSI

Ambiente de SI/TI	Departamento	Nº Colaboradores	Responsável
Todos os sistemas em âmbito	Departamento de sistemas de informação	20	Diretor do DSI
Todos os sistemas em âmbito	Subdireção de comunicação e desenvolvimento	11	Diretor da subdireção de comunicação e desenvolvimento
Todos os sistemas em âmbito	Subdireção de *helpdesk*	4	Diretor do *helpdesk*
Todos os sistemas em âmbito	Subdireção de administração de sistemas	5	Diretor da subdireção de administração de sistemas

Caracterização das áreas dos controlos de SI/TI

Gestão de operações (rede e CPD)

Processos *job/batch*

Não se encontra definido/ formalizado um procedimento de gestão de operações (gestão de *jobs/batchs*) que inclua os processos *job/batch* existentes (nomeadamente os de maior criticidade), as normas e orientações relacionadas com a aprovação/ calendarização de *jobs/batchs,* assim como os procedimentos e responsáveis pela sua monitorização e correção.

Apesar de não formalizado o procedimento formal para os sistemas em âmbito, descreve-se a seguir como se realiza a gestão das operações na operadora:

Sistema Cobranças e Contabilidade

O processamento dos *jobs/batches* de ambos os sistemas (Cobranças e Contabilidade) é, realizado a partir de alertas (via email). A monitorização dos *jobs/batches* é realizada pela DSI. Sempre que ocorre um erro que a DSI não tem *know-how* suficiente, recorre a um fornecedor externo de apoio aos sistemas. Adicionalmente, o processamento dos *jobs/batches* é registado em *logs*, sempre que ocorre um erro a DSI analisa o *log* para auxiliar a resolução do mesmo. No entanto, a DSI não realiza qualquer relatório mensal da correção dos erros do processamento dos *jobs/batches.*

Sistema *Billing* GSM

Os *jobs/batches* do sistema *billing* GSM são geridos e monitorizados pelo parceiro de negócio da operadora, não sendo reportado qualquer relatório à operadora de monitorização dos *jobs/batches* do sistema *billing* GSM, bem como a correção de erros.

Backups

Não está formalmente definido/ documentado o procedimento de gestão de *backups*, que inclua, entre outros, a estratégia de *backups*, período de retenção, monitorização de *backups*, rotação de tapes para localização *off-site.*

Apesar de não formalizado o procedimento formal para os sistemas em âmbito, descreve-se a seguir como é feita a gestão de *backups* na operadora:

- Sistemas Cobranças e Contabilidade:

Existe uma rotina de *backup* para o sistema Cobranças e duas rotinas de *backup* para o sistema Contabilidade, sendo todas as rotinas totais e diárias. Os *backups* são efetuados para tape, com um período de retenção de 15 dias.

Os *jobs* dos *backups* são monitorizados, diariamente através dos *logs* gerados pelos sistemas, por dois responsáveis da DSI. Quando ocorrem erros, estes analisam e tentam resolver o problema, se não tiverem o *know-how* suficiente, recorrem a um fornecedor externo. No entanto, a DSI não realiza qualquer relatório mensal da correção dos erros do processamento dos *jobs* de *backup*.

- Sistema *billing* GSM:

Fomos informados que os jobs dos *backups* são monitorizados pelo parceiro de negócio da operadora, não sendo reportado qualquer relatório à operadora de monitorização dos *jobs* de *backup* do sistema *billing* GSM, bem como a correção de erros.

Adicionalmente, não se encontra definido e implementado um plano de *disaster recovery plan* (DRP) e *business coninuity planing* (BCP), tal como não é realizado o armazenamento *off-site* das tapes de *backups*.

Helpdesk

Os pedidos de *helpdesk* (e.g. problemas nas impressoras, *reset* de *passwords*) são realizados por email ou telefone, nestes casos a DSI analisa a situação e procede à sua resolução.

Monitorização de rede

A monitorização de rede é realizada através da utilização da ferramenta Nagios. A ferramenta permite a monitorização de infraestruturas de SI/TI (e.g. detetar falhas de segurança de rede; e monitorizar disponibilidade do sistema).

Gestão de segurança de informação

Segurança lógica

Políticas e procedimentos

Encontra-se definida/ formalizada uma política empresarial de segurança da informação alinhada com as boas práticas de mercado, na qual deveriam ser considerados os sistemas de informação, as instalações e a proteção dos recursos humanos.

Quanto ao *software* de antivírus, a operadora tem um produto da McAfee, que se encontra instalado num servidor centralizado, efetua *updates* diários e faz o *deployment* para as estações de trabalho. Esta ferramenta permite a elaboração de relatórios de monitorização.

Não existem procedimentos formalizados que definam uma nomenclatura de utilizadores e que reflita as práticas utilizadas informalmente na operadora.

A operadora não possui um programa de comunicação e sensibilização dos utilizadores relativamente à segurança de informação, nem ao modo como a informação deve ser manuseada.

Gestão de acessos

Não existem procedimentos formalizados de gestão de acessos (criação, alteração e remoção) aos sistemas de informação.

Apesar disso, quando é admitido um novo colaborador, o responsável de RH (com conhecimento do responsável da área) envia um email para o diretor da DSI a solicitar o acesso à rede e aos sistemas, com a definição do tipo de acesso pretendido.

Quando é necessário efetuar uma alteração ao perfil de um utilizador, o responsável da área do colaborador envia um email ao diretor da DSI a solicitar a alteração do acesso e definição do novo perfil.

Relativamente à remoção de utilizadores nos sistemas, sempre que um colaborador deixa de trabalhar na operadora, os recursos humanos (RH) enviam um email ao diretor da DSI, com essa informação. Após receção desse email, o diretor da DSI procede à desativação do utilizador na rede e sistemas.

Revisão de acessos

Não é efetuada periodicamente uma revisão aos utilizadores e respetivos perfis, com o objetivo de identificar utilizadores genéricos, duplicados, colaboradores que saíram da operadora, perfis inadequados às funções dos utilizadores, entre outros.

Não se encontra definida uma matriz de segregação de funções da operadora que sirva de base à definição dos perfis de acesso implementados nos sistemas em âmbito, não sendo validada a possibilidade de atribuição de acessos, com eventuais conflitos críticos.

Acessos externos

Maioritariamente, os acessos externos são atribuídos a colaboradores, que operam com os sistemas, nomeadamente:

Tabela 11 – Acessos externos

Quem tem acesso?	Propósito do acesso
Administradores de sistemas	Acesso necessário para monitorização e resolução de problemas remotamente. Os acessos são efetuados via VPN para os membros do DSI (*remote access*), de modo a que os mesmos tenham acesso aos servidores onde correm os sistemas.

A operadora tem uma *firewall* configuradas na sua rede gerida e parametrizadas pela DSI:

Tabela 12 - *Firewall* da operadora

Método de proteção	Descrição
***Firewall* (Cisco)**	Controlo realizado pelo departamento de sistema de informação.

Segurança física

Acessos físicos

Verificámos que não se encontra definida/ formalizada uma política empresarial de segurança da informação alinhada com as boas práticas de mercado, na qual deveriam ser considerados os sistemas de informação, as instalações e a proteção dos recursos humanos.

O acesso ao edifício é controlado através de seguranças, que se encontram na receção, sendo o acesso efetuado através de cartão de identificação (com fotografia).

O acesso ao centro de processamento de dados (CPD) é realizado através de cartão magnético, onde se encontram localizados os servidores dos sistemas de Cobranças e Contabilidade, efetuado com cartão magnético, no entanto, existe um registo em *logs* desses acessos.

Relativamente ao acesso físico ao CPD por parte de visitantes/ fornecedores externos, é efetuado através do acompanhamento feito por um dos colaboradores com acesso.

A responsabilidade da atribuição e recolha dos cartões magnéticos que permitem o acesso físico ao CPD é da responsabilidade da administração da operadora. No entanto, não estão formalmente definidos procedimentos de gestão e controlo dos acessos físicos.

Os métodos utilizados para segurança física são sintetizados da seguinte forma:

Tabela 13 - Resumo acessos físicos

Dispositivo de acesso	Localização
Cartão de identificação	Edifício Sede
Cartão magnético	Centro de processamento de dados (CPD)

A Tabela 14 abaixo, lista todos os grupos (internos e externos) que têm permissão de acessos físicos aos locais restritos da operadora:

Tabela 14 – Grupos de acessos físicos

Local	Grupo	Natureza das restrições de acesso
Edifício Sede	DSI	Acesso total
	Colaboradores	Acesso total
	Acessos de externos	Acesso restrito acompanhado por responsável

CPD	DSI	Acesso total
	Colaboradores	Acesso restrito acompanhado por responsável
	Acessos de externos	Acesso restrito acompanhado por responsável

Caracterização da gestão de alterações

Está formalmente descrito o procedimento de gestão de alterações que descreve as seguintes principais fases e responsabilidades: (i) Definição de requisitos; (ii) Análise e aprovação; (iii) Desenvolvimento; (iv) Testes (e.g. de carga, técnicos, de aceitação); e (v) Aprovação da passagem a produção.

O procedimento documentado instituiu a seguinte metodologia: o pedido de desenvolvimento é realizado junto da DSI é efetuado com recurso ao email já após a aprovação do responsável de negócio. Após o pedido é efetuada uma análise de requisitos e viabilidade incluindo o tempo e custo para o desenvolvimento.

Caso o projeto seja aceite, avança-se e a DSI notifica o fornecedor externo de apoio aos sistemas, para proceder à alteração. Quando a alteração já se encontra efetuada são realizados testes, sendo estes aprovados pelos *key-users* antes da passagem a produção.

Adicionalmente, as alterações ao sistema *Billing* GSM, são da total responsabilidade do parceiro de negócio. No entanto, todas as alterações realizadas ao sistema *Billing* GSM têm de ser notificadas e aprovadas pelo PMO (*Project Management Office*) da operadora.

Sistema Operativo

Verificámos que não se encontram formalizados e documentados os procedimentos de instalação e realização de testes, antes da instalação em produção de *updates/ patches* do sistema operativo.

Apesar de não existir um procedimento definido/ documentado, quando existem novos *updates/ patches* comunicados pelo fornecedor (Microsoft), a DSI faz as atualizações de acordo com as especificações fornecidas pelo fornecedor.

Bases de dados

As alterações às bases de dados são, por norma, realizadas no âmbito de alterações aplicacionais, sendo geridas no âmbito destas e de acordo com o procedimento de gestão de alterações definido/ implementado.

4.7. Identificação dos riscos

Nesta secção encontra-se descrita a identificação dos riscos, bem como os riscos que foram/ podem ser mitigados com a realização do presente trabalho

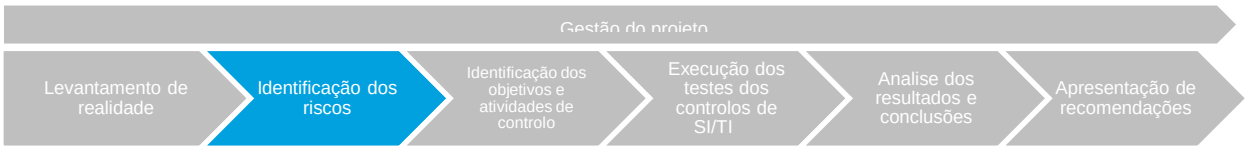

Imagem 30 - Fase identificação dos riscos

Depois do conhecimento do negócio da operadora, é necessário identificar os riscos associados à correta captação da receita, foram usadas as seguintes fontes de informação:

- Consulta do mapa de riscos RIM (explicado na secção 3.2.1 do presente relatório), selecionando os riscos que se aplicavam à realidade da operadora; e
- Com base no conhecimento do negócio da operadora.

A identificação dos riscos associados aos sistemas de informação é um dos pontos mais fulcrais do trabalho, pois estes são o ponto de partida para as análises efetuadas aos sistemas de informação, ou seja, é a partir destes riscos que são definidos os objetivos de controlo, atividades de controlo e respetivos testes, conforme está apresentado na Imagem 31.

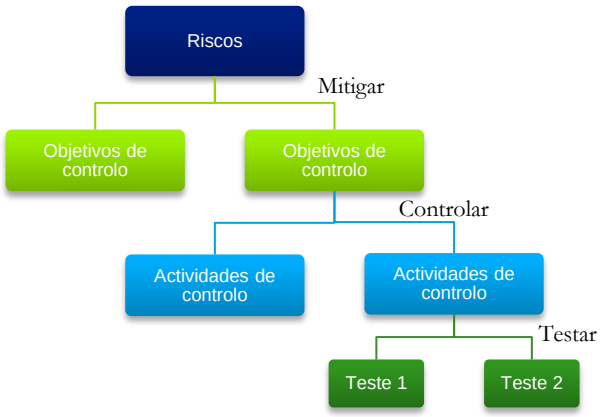

Imagem 31 - Árvore de mitigação de risco

Podendo estes ser divididos pelas seguintes variantes:

- Risco de operações - serem ineficientes ou ineficazes na satisfação dos clientes e no alcance dos objetivos da empresa.
- Riscos de "*empowerment*" - os riscos inerentes aos processos de delegação de competências e responsabilidades.

- Riscos tecnológicos/ processamento da informação - o risco de que as tecnologias de informação não apoiem eficaz e eficientemente as necessidades atuais e futuras do negócio, pondo em risco a salvaguarda de ativos, informação e as operações da empresa.
- Riscos de integridade - os riscos de fraude da gestão ou de empregados, e de ocorrência de atos ilegais ou não autorizados, que possam comprometer a reputação da empresa.
- Riscos financeiros - incluem um largo espectro de riscos que a empresa enfrenta diariamente; a sua gravidade depende de vários fatores que incluem a dimensão da empresa, sector de atividade, situação financeira, e a direção do mercado.

Como já foi referido na secção 4.1 do presente relatório, o objetivo do trabalho é garantir a correta captação da receita. Para isso, foi necessário identificar os riscos associados a este objetivo. A identificação dos riscos passou por duas fases de seleção, nomeadamente:

- A primeira fase consistiu em identificar os riscos associados à receita da operadora, para todos os processos. A identificação dos riscos teve como base o RIM; e
- A segunda fase passou por uma reunião com o concelho de administração, onde a equipa da Deloitte, apresentou os riscos identificados. A administração, com os resultados dos testes de integração, determinou que seria necessário mitigar os riscos associados aos sistemas de informação associados ao processamento da faturação.

No **anexo 2**, encontram-se os riscos identificados, relativos ao ciclo de receita, bem uma breve descrição.

4.8. Identificação dos objetivos e atividades de controlo

Estando os riscos identificados é agora necessário definir os objetivos de controlo e as atividades de controlo, necessários para mitigar os riscos.

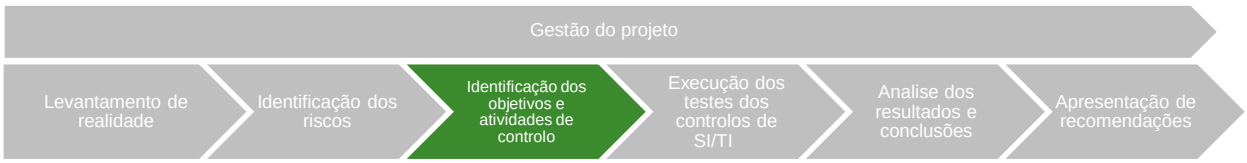

Imagem 32 - Fase identificação OCs e ACs

Objetivos de controlo (OC)

Após os riscos identificados, é necessário responder à seguinte pergunta:

Como é que vamos controlar os riscos?

Os riscos são controlados a partir dos objetivos de controlo. Sendo agora necessário identificá-los, de forma a controlar o risco anteriormente identificado. Os objetivos de controlo foram identificados através de três vias, tal como apresenta a seguinte imagem:

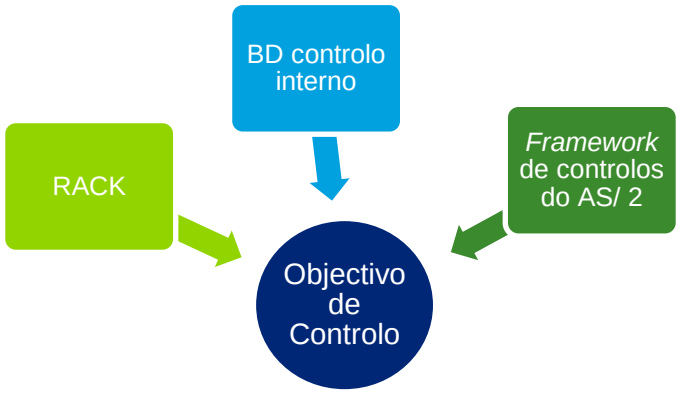

Imagem 33 - Fatores que definem os objetivos de controlo

Os objetivos de controlo foram determinados a partir das três vertentes que se encontram acima apresentadas, sendo estas as seguintes:

- **RACK**: como já referido na seção 3.2.1 do presente relatório, é a lista que contém vários objetivos de controlo, de onde é possível selecionar os que se adequam à mitigação dos riscos identificados anteriormente;
- **Base de dados de controlo interno**: inclui objetivos de controlo, identificados com base numa base de dados de controlo interno do cliente descrita em iniciativas anteriores; e
- **Framework de controlos do AS/2** (ferramenta de documentação de auditorias da Deloitte): documentação que a Deloitte produziu em auditorias anteriores, onde os mesmos riscos possam ter ocorrido.

Atividades de controlo (AC)

Depois dos objetivos de controlo identificados, temos voltar a fazer uma pergunta:

Como é que vamos alcançar os objetivos de controlo?

Para alcançarmos cada objetivo de controlo é necessário identificar que atividades são ou devem ser realizadas na operadora de modo a alcançar os objetivos de controlo anteriormente definidos.

Estas atividades são realizadas no dia-a-dia da empresa e são estas que garantem que à operadora, ao realizá-las, o cumprimento e resposta aos objetivos de controlo.

Algumas atividades de controlo foram identificadas também com a ajuda do RACK. Estando os objetivos de controlo determinados, podemos pesquisar no RACK as atividades de controlo que correspondem a estes e adequá-los à nossa realidade.

No **anexo 3**, encontram-se os riscos dos sistemas em âmbito, com os respetivos objetivos e atividades de controlo associados. Nesta tabela, todos os riscos, OC e AC foram devidamente detalhados, de forma a mapear com a realidade da operadora.

4.9. Execução dos testes dos controlos de SI/TI

Estando os processos de negócio e de suporte dos SI/TI levantados, assim como os riscos, os objetivos de controlo e as atividades de controlo, é agora necessário desenhar os testes.

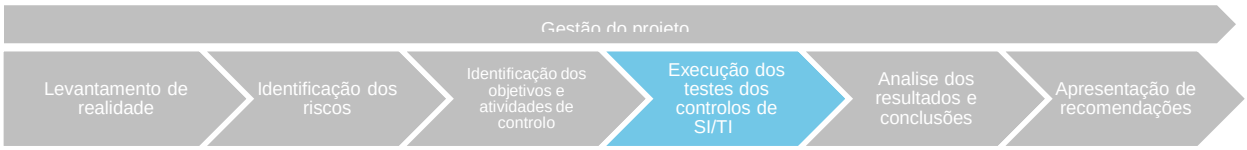

Imagem 34 - Fase teste dos controlos de SI/ TI

O desenho dos testes tem como objetivo analisar se atividades de controlo estão a ser devidamente aplicadas/ realizadas na operadora. Tal como já foi referido anteriormente, para cada atividade de controlo, pode haver um ou mais testes, para garantir que a atividade existe ou não. Caso exista, é necessário garantir que esta está a ser devidamente de forma a alcançar os objetivos de controlo.

No **anexo 5**, está apresentada uma a matriz de testes, com a descrição de cada teste, bem como a informação necessária para a realização do mesmo.

Pedido de informação

Tal como foi explicado na secção 3.2.3 do presente relatório, o pedido de informação foi realizado com base nos testes anteriormente definidos. Para cada teste, foi necessário identificar toda a informação necessária para a realização do mesmo. No **anexo 4**, encontram-se os pedidos solicitados à operadora para a realização dos testes.

4.9.1. Testes dos controlos de SI

Esta secção tem como objetivo explicar de uma forma macro, a realização dos testes que estão descritos no **anexo 5**.

A explicação dos testes, será disposta tal como se apresenta na matriz de testes e dividida por objetivo de controlo, nomeadamente:

- Geral

O teste realizados para os fornecedores externos consiste em:

- [FOR.01] - Garantir que o contrato entre a operadora e o parceiro de negócio se encontra em vigor:

- Analisar quais as responsabilidades por parte do fornecedor externo, relativamente aos sistemas; e
- Analise dos contratos entre o fornecedor externo e a operadora, de forma a verificar se estes se encontram em vigor.

- Gestão de operações

Os testes realizados para a gestão de operações consistem em:

- [OPER.01] – A gestão de operações é apropriada para suportar a calendarização, execução, monitorização, e continuidade dos programas e processos de SI/TI para um completo, eficiente e valido processamento e registo das transações:
  - Análise dos procedimentos dos controlos dos *jobs/ baches*. Em caso de não existir um procedimento documentado, é necessário entender juntamente com a DSI como é realizado o controlo dos *jobs/ batches* e realizar a avaliação;
  - Análise da calendarização dos *jobs/batches*. A partir da análise à calendarização, é possível verificar quais os *jobs/ baches* que são executados, e realizar a análise;
  - Análise dos registos de execução dos *jobs/ bacthes*. Com a informação recebida, é possível verificar se existiu algum erro de processamento. No caso de erros, são solicitados a correção dos mesmos; e
  - Análise dos procedimentos realizados no tratamento de erros de execução dos *jobs/ bacthes*.

- [OPER.02] - Os dados são geridos de forma a assegurar que a informação se mantém completa, correta e valida durante o processo de *backup*, de forma a estar assegurado a recuperação da informação em caso de necessidade:
  - Análise dos procedimentos realizados no tratamento de erros de execução dos *backups*. Em caso de não existir um procedimento implementado na operadora, é necessário entender juntamente com a DSI como é realizado o controlo dos *backups* e realizar a avaliação;
  - Análise da calendarização dos *backups*. A partir da calendarização é possível identificar os *backups* que são realizados, bem como a sua periodicidade;
  - Análise dos registos de execução dos *backups*. Com a informação recebida, é possível verificar se todos os *backups* que estão definidos na calendarização estão a ser devidamente executados, bem como verificar se ocorreu algum tipo de erros de processamento; e
  - Análise da correção realizada aos erros de processamento dos *backups*.

- Gestão dos sistemas de informação

Os testes realizados para a gestão dos sistemas de informação consistem em:

- [SEG.01] - A segurança dos sistemas é corretamente implementada, administrada e registada de forma a evitar o acesso/ modificações de programas ou dados que resultem num incompleto, incorreto ou invalido processamento/ registo da informação:
    - Análise da política de segurança de informação implementada na operadora. Em caso desta não existir, é necessário entender juntamente com a DSI, quais os procedimentos implementados na empresa, tais como: nomenclatura dos utilizadores; quais os perfis têm acesso alargado aos sistemas; parâmetros de autenticação; e procedimentos de admissão/ remoção/ alteração de utilizadores;
    - Análise ao procedimento de revisão de acessos implementado na operadora. Se não existir um procedimento formal, é necessário perceber juntamente com a DSI, se é realizado alguma revisão e como esta é executada;
    - Análise à política de gestão de acessos físicos às instalações e ao CPD. Em caso de não existir é necessário entender os procedimentos realizados aos acessos físicos às instalações e ao CPD da operadora;
    - Análise aos utilizadores que cessaram funções com a operadora no ano de 2014. Nos pontos anteriores foi avaliado o procedimento de remoção de utilizadores. Com o presente teste é necessário verificar que o procedimento de remoção está a ser devidamente aplicado na operadora;
    - Análise aos utilizadores que cessaram funções com a operadora no ano de 2014. O teste consiste em mapear as listagens de utilizadores dos sistemas em âmbito e AD, de forma a verificar se não existem utilizadores ativos nos sistemas que já tenham cessado funções com a operadora;
    - Análise à revisão de acessos aos utilizadores. O teste consiste em verificar se a operadora realiza qualquer validação aos acessos que estão fornecidos aos utilizadores (e.g. se a função do colaborador necessita que este tenha acessos alargados ao sistema);
    - Análise da matriz de segregação de funções. O teste consiste em verificar se as funções aos utilizadores estão de acordo com a matriz de segregação de funções, bem como ver se a matriz está devidamente implementada entre as funções de cada utilizador.

- [SEG.02] - As configurações de segurança de programas e sistemas são geridas de forma eficiente para prevenir alterações, a programas e dados, não autorizadas que possam por em risco o completo e correto processamento de informação:
    - Análise da listagem de utilizadores incluindo os respetivos perfis de acessos. O teste consiste em analisar os utilizadores com acessos alargado. Validar que o acesso alargado apenas está associado a utilizadores que necessitam para desempenhar as suas funções;

      Adicionalmente, verificar se existem utilizadores genéricos (e.g. utilizador: user01).

- Análise da listagem dos utilizadores com acesso direto às bases de dados (acesso de escrita na base da dados) de apoio aos sistemas em âmbito;
- Análise aos parâmetros de seguranças dos sistemas em âmbito e *Active Directory*. O teste consiste em validar que os parâmetros de segurança estão de acordo com a política de segurança da empresa e com as melhores práticas; e
- Verificar que a operadora tem um *software* de antivírus instalado e que está devidamente atualizado. Adicionalmente verificar que existem *scans* periódicos aos computadores da operadora.

- [SEG.03] - Os acessos físicos são geridos de forma a proteger a integridade da informação e garantir que esta é mantida e guardada com recurso aos componentes corretos da infraestrutura de tecnologias de informação:
  - Análise ao procedimento de controlo de acessos físicos. No caso da operadora não contenha um procedimento formal documentado, é necessário realizar o entendimento juntamente com a DSI, de forma a validar os controlos realizados;
  - Análise aos acessos aos CPD, este teste consiste em verificar que os acessos são devidamente registados e que apenas acedem colaboradores com permissão provada; e
  - Análise às revisões de acessos ao CPD, de forma a verificar que os *logs* de acesso e os colaborados com permissões de entrada, são revistos.

- [SEG.04] - O sistema é resiliente a falhas catastróficas, acidentais ou intencionais:
  - Análise ao plano de continuidade de negócio e um plano de recuperação de desastres. O teste consiste em validar os planos e verificar que estes englobam todos os pontos necessários; e
  - Realizar uma visita presencial ao CPD, para verificar que este engloba todas as medidas de segurança necessárias para contemplar a segurança física do CPD.

- Gestão de alterações

Os testes realizados para a gestão de alterações consistem em:

- [ALT.01] - Os programas e sistemas são adequadamente modificados para suportar o processamento e registo da informação de forma correta, completa e válida:
  - Analisar a metodologia ou processo de modificação dos sistemas aplicacionais. No caso de não existir, é necessário reunir com a DSI da operadora, por forma a entender e a documentar o processo de alterações utilizado na operadora;
  - Analisar as alterações realizadas às aplicações, bases de dados e sistema operativo. A partir da listagem de alterações existem três componentes a avaliar, nomeadamente:
    - Se existe uma aprovação formal da alteração/ desenvolvimento;
    - Se foram efetuados testes após o desenvolvimento;
    - Se existe uma aprovação formal dos teste e da entrada em produção; e

- Se foram realizados testes aos *patches* do sistema operativo antes da instalação em produção.

Todos os testes encontram-se descritos no **anexo 5**, com a respetiva informação necessária para a sua realização e conclusão.

4.9.2. Testes de integração da informação

Nesta secção estão descritos os testes de periódicos, sendo estes utilizados para verificar a correta integração da receita, relativamente aos carregamentos e consumos.

Os testes periódicos realizados aos carregamentos e aos consumos, têm como objetivo verificar a correta integração dos carregamentos e dos consumos de saldo, em números pré-pagos na rede GSM, na contabilidade, mais concretamente no *billing* contabilidade. Estes testes foram desenhados com o objetivo de garantir que a integração da receita nos sistemas é bem efetuada. Os principais objetivos desta análise dos carregamentos e consumos de números pré-pagos GSM são os seguintes:

- Verificar a correta extração da informação de carregamentos e dos consumos de saldo em números pré-pagos GSM, do sistema de billing GSM;
- Aferir o correto reflexo contabilístico dos carregamentos e consumos de saldo em números pré-pagos GSM, no sistema de *billing* contabilidade
- Identificar as situações de exceção e as necessidades de correção; e
- Acompanhar a implementação de medidas de correção e ajustamento.

Através dos testes periódicos temos como objetivo realizar a validação da integridade dos dados entre o sistema de *billing* GSM e Contabilidade na integração da informação dos carregamentos e consumos de saldo em números pré-pagos GSM, tal como ilustrado na seguinte Imagem 35:

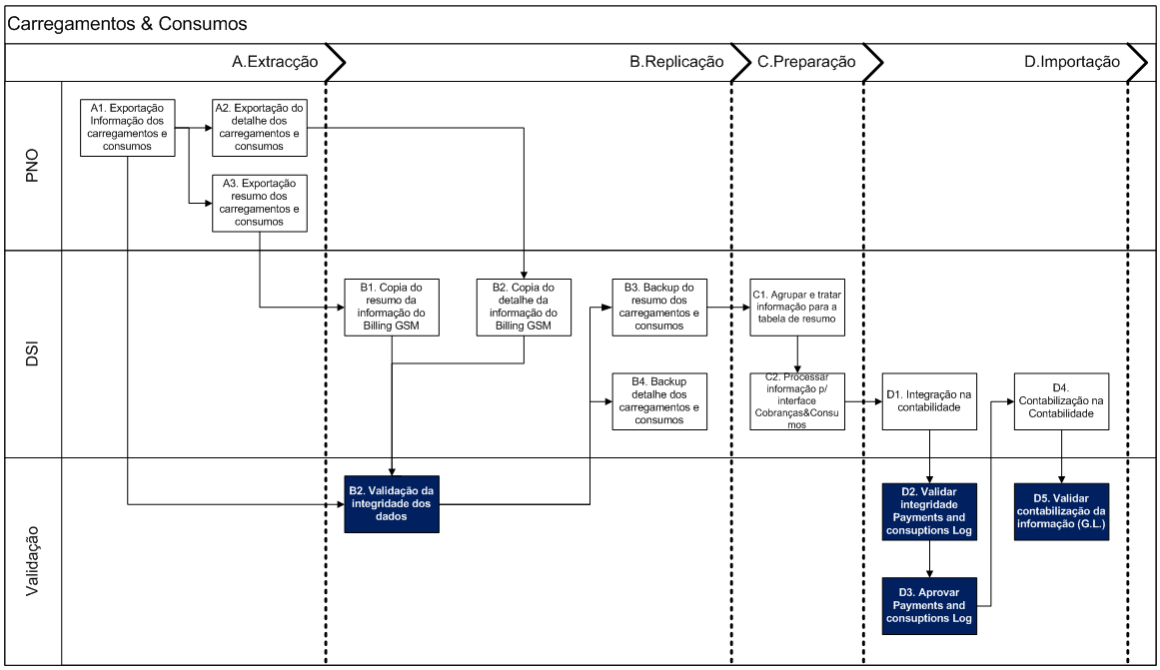

Imagem 35 - Importação dos números pré-pagos GSM

Carregamentos

Os carregamentos são realizados pelos clientes da operadora de telecomunicações. Os clientes podem adquirir estes cartões pré-pagos em qualquer estabelecimento proprietário da operadora, bem como a qualquer revendedor. Esses cartões podem diferir consoante a quantidade de saldos que o cliente deseja. Quando este é adquirido, basta ver o código contido no seu interior e enviar uma mensagem de texto com o respetivo código, e automaticamente o saldo fica disponível no cartão do cliente. Existe ainda outra maneira de carregar o telemóvel, bastando o cliente efetuar um carregamento num multibanco, e este fornece um código, sendo o processo realizado de igual modo.

[B2] Validação da integridade dos dados do *Billing* GSM

A primeira atividade é realizar a validação da integridade dos dados extraídos do *billing* GSM no processo de integração da informação de carregamentos de saldo em números pré-pagos GSM na contabilidade. Tendo como objetivos, garantir que os dados dos carregamentos de saldos dos números pré-pagos GSM, foram extraídos do sistema de *billing* GSM para integração na contabilidade, sendo verificados os seguintes pontos:

- Se o período de faturação corresponde ao correto e se inclui todos os dias do período de faturação; e
- Se os dados dos carregamentos de saldo de números pré-pagos GSM estão registados corretamente no sistema de *billing* GSM.

- Para a execução, desta validação são necessários os seguintes dados:

1. Produtos/ eventos de carregamento e de comunicação registados no sistema de billing GSM, sendo estes fornecidos pelo PNO, contendo a identificação e o nome dos produtos/ eventos dos carregamentos no sistema billing GSM;
2. Tabela com o resumo dos carregamentos de saldo em números pré-pagos GSM, que foram extraídos do sistema de *billing* GSM, para integração na contabilidade;
3. Tabela com o detalhe dos carregamentos de saldo em números pré-pagos GSM, que foram registados no sistema de *billing* GSM.

Procedimento:

A validação da integridade dos dados contidos no sistema de *billing* GSM, no processo de integração de carregamentos de saldo dos números pré-pagos GSM na contabilidade, realiza-se com a reconciliação dos dados entre as tabelas dos pontos 2 e 3. A validação é realizada com a execução dos seguintes passos:

- Carregamento da informação, ou seja, integração das tabelas no ACL;
- Validação do período considerado, isto é, verificar se ambas as tabelas se encontram no período de faturação correto;
- Comparação entre as duas tabelas, sendo estas filtradas apenas por números pré-pagos e verificar se existem diferenças nos valores de carregamentos de alguns produtos/ eventos.

[D2] Validação de integridade do Log Cobranças & Consumos

A segunda atividade é a realização da validação dos dados dos carregamentos de saldo em números pré-pagos GSM na interface de Cobrança & Consumos, para garantir que estes dados são resultantes do processo de preparação da informação para a integração na contabilidade, são os dados que se encontram registados e extraídos do sistema de *billing* GSM. Para a execução desta validação são necessários os seguintes dados:

1. Produtos/ eventos de carregamento e de comunicação registados no sistema de *billing* GSM, sendo estes fornecidos pelo PNO, contendo a identificação e o nome dos produtos/ eventos dos carregamentos no sistema de *billing* GSM;
2. Tabela com a informação dos recursos que foram integrados na contabilidade;
3. Tabela de mapeamento entre os dois sistemas de *billing*;
4. Tabela dos produtos a excluir antes de integrarem na contabilidade;
5. Tabela com o resumo dos carregamentos de saldo em números pré-pagos GSM extraídos do sistema de *billing* GSM para integração no sistema contabilidade; e
6. Log da interface de integração das cobranças e dos consumos, na contabilidade. Aqui são armazenados, entre outros, os documentos NPP (faturas dos consumos relativamente aos clientes de números pré-pagos) gerados com a informação de carregamentos de saldo em números pré-pagos GSM, prontos para serem contabilizados.

Procedimento:

A validação da integridade dos dados de carregamento de saldo nos números pré-pagos GSM que se encontram em condições para serem integrados na contabilidade, no Log de *Cobranças & Consumos* no sistema de *billing* contabilidade, realiza-se fazendo a comparação entre os dados das tabelas 5 e 6. A validação é realizada com a execução dos seguintes passos:

- Importação das tabelas no ACL;
- Cruzamento da informação:
    - Realização de um filtro na tabela 5, de modo a filtrar os números pré-pagos;
    - Realização de um filtro na tabela 6, de modo a apenas considerar apenas os produtos/ eventos que foram integrados;
    - Juntar a tabela 3 (mapeamento de produtos do *billing* GSM, à tabela 5 já filtrada com o resumo dos carregamentos);
    - Juntar as duas tabelas geradas nos últimos dois pontos e se existe diferenças monetárias entre o *billing* GSM e a contabilidade.
    - Juntar a tabela 2 com a que foi gerada anteriormente, de forma a gerar uma tabela com todos os detalhes; e
    - Verificar se existem diferenças nos valores de carregamentos de alguns produtos/ eventos de carregamento.

[D3] Aprovação Log *Payments* & *Consumptions*

A terceira atividade tem como objetivo realizar a aprovação da integridade e contabilização dos dados dos carregamentos efetuados pelos clientes com números pré-pagos GSM, na "General Ledger", que se encontra na contabilidade. Para isso é necessário garantir que os dados de carregamentos de saldo nos números pré-pagos GSM, refletidos nas rúbricas da contabilidade, sejam validados antes de serem contabilizados de modo a ver se se encontram íntegros e se se enquadram nas expectativas da área financeira. Para a execução desta validação, são necessários os seguintes dados:

1. Tabela com a lista de recursos que foram integrados na contabilidade;
2. Log da interface de integração das cobranças e dos consumos, na contabilidade. Aqui são armazenados, entre outros, os documentos NPP gerados com a informação de carregamentos de saldo em números pré-pagos GSM, prontos para serem contabilizados. Com esta informação terão de ser duas tabelas, uma relativamente ao mês que se está a analisar e outra com o mês anterior.

Procedimentos:

A validação da integração e contabilização dos dados dos carregamentos de saldo relativamente aos números pré-pagos GSM, na General Ledger, na contabilidade, realiza-se através da comparação entre os dados dos carregamentos a integrar do mês que se está a avaliar e o mês anterior, sendo necessário realizar as seguintes ações:

- Importar todas as tabelas que foram referidas anteriormente no ACL;
- Cruzamento da informação:
    - Filtrar das tabelas do ponto 2, apenas os produtos/ eventos que foram integrados;
    - Juntar as tabelas, apenas com os dados mais relevantes, bem como o cálculo da diferença dos carregamentos de saldo entre os dois meses em análise;
    - Juntar a tabela que foi realizada no ponto anterior, com a lista de recursos que foram integrados na contabilidade; e
    - Analisar as diferenças e aprovar a integração e contabilização dos carregamentos de saldo em números pré-pagos GSM na contabilidade.

[D5] Validação contabilização da informação

A última atividade tem como objetivo realizar a validação dos dados dos carregamentos de saldo para os números pré-pagos GSM na contabilidade, mais concretamente na "General Ledger", tendo então que garantir que estes dados se encontram refletidos nas rubricas de contabilidade (e.g. os valores são iguais aos que estão na interface anterior e as rubricas atualizadas foram as validadas).Para a execução desta validação são necessários os seguintes dados:

1. Tabela com a informação dos recursos que foram integrados na contabilidade;
2. Tabela *Paymentand Consumptions Log* da interface de integração das cobranças e dos consumos, na contabilidade, sendo armazenados, entre outros, os documentos NPP gerados com a informação de carregamentos de saldo em números pré-pagos GSM, prontos para serem contabilizados; e
3. Tabela "General Ledger", sendo o local onde são registados todos os registos contabilísticos que se encontram a afetar as rubricas contabilísticas.

Procedimento:

A validação da contabilização dos dados de carregamentos de saldo em números pré-pagos GSM na contabilidade, mais concretamente na General Ledger, é realizada através da comparação entre os dados das tabelas do ponto 2 e 3. A validação é realizada com o auxílio da ferramenta ACL para a execução dos seguintes passos:

- Importação no ACL das três tabelas anteriormente apresentadas;
- Validação dos pressupostos assumidos na análise à integridade da informação na General Ledger:
    - Cada documento NPP de carregamentos de saldo em números pré-pagos GSM apenas tem uma linha de detalhe;
    - Cada documento NPP de carregamentos de saldo em números pré-pagos GSM apenas gera uma transação no processo de contabilização na General Ledger;

    - Cada NPP/ transação só gera 2 linhas na General Ledger;
    - Na General Ledger, cada uma das duas linhas de cada NPP/ transação comporta a mesma informação:
- Separar em duas tabelas as linhas que têm valores a crédito e as que têm valores a débito;
- Criação de uma nova tabela, para realizar a separação do crédito e do débito, de forma que esta informação fica apenas numa linha, através do identificador do documento;
- Validar que as linhas contêm a mesma informação:
    - Conta a crédito da 1ª (número de conta da GL) é igual à conta a débito na segunda (número de conta do balancete);
    - Conta a débito da 1ª (número de conta do balancete) é igual à conta a crédito na 2ª (número de conta da GL);
    - O valor (Quantidade) da 1ª é simétrico ao da 2ª;
    - O valor a crédito da 1ª é igual ao valor a débito na 2ª; e
    - O valor a crédito da 2ª é igual ao valor a débito na 1ª.

- Comparação da informação, este processo é realizado manualmente utilizando todas as tabelas que foram geradas anteriormente, como ferramenta foi utilizado o Microsoft Excel:
    - Juntar as tabelas *Generel Ledger* e a *Paymentsand Consumptions Log*, através do identificador do documento da interface;
    - Com a tabela que foi gerada no ponto anterior, juntar a tabela de *Resources*, de modo a criar uma nova tabela os pontos essenciais à nossa análise, bem como acrescentar uma coluna com a diferença entre o que se encontra na contabilidade e na interface.
    - Verificar se existem diferenças nos valores de carregamentos de alguns produtos/ eventos de carregamentos, nas rúbricas de contabilidade.

Consumos

Os consumos são bastante idênticos aos carregamentos. Nesta secção apenas serão explicadas as fases que diferem dos carregamentos. Relativamente à extração e importação da informação o método é o mesmo, tal como exemplifica a Imagem 35.

[B2] Validação da integridade dos dados do sistema de Billing GSM

A primeira atividade é realizar a validação da integridade dos dados extraídos do *billing* GSM no processo de integração da informação dos consumos de saldo em números pré-pagos GSM na contabilidade. Tendo como objetivos garantir que os dados dos consumos de saldos dos números pré-pagos GSM, que foram extraídos do sistema de *billing* GSM para integração na contabilidade, sendo verificados os seguintes pontos:

- Se o período de faturação corresponde ao correto e se inclui todos os dias do período de faturação; e se os dados dos consumos de saldo de números pré-pagos GSM estão registados corretamente no sistema de *billing* GSM.

Para validação dos consumos obtemos:

1. Listagem de produtos/ eventos dos consumos das comunicações que foram registados no sistema de *billing* GSM, sendo estes fornecidos pelo PNO, contendo a identificação e o nome dos produtos/ eventos dos carregamentos no sistema *billing* GSM;
2. Tabela com o resumo dos consumos de saldo em números pré-pagos GSM extraídos do sistema de *billing* GSM, para integração na contabilidade; e
3. Tabela com o detalhe dos consumos de saldo em números pré-pagos GSM, que foram registados no sistema de *billing* GSM.

Procedimento:

A validação da integridade dos dados do sistema de *billing* GSM, no processo de interação da informação de consumos de saldo em números GSM na contabilidade, é realizada através da comparação entre as tabelas dos pontos 2 e 3. A validação é realizada com a execução dos seguintes pontos, através de scripts em ACL e posteriormente passados para Excel, para análise final:

- Importação de todas as tabelas, no ACL;
- Validação do período considerado, isto é, verificar se as datas se encontram dentro do período de faturação;
- Comparação da informação:
    - Filtrar as duas as tabelas (resumo e detalhe) dos consumos, apenas para números pré-pagos;
    - Juntar as duas tabelas anteriores;
    - Juntar à tabela do ponto anterior a listagem de produtos; e
    - Verificar e existem diferenças nos valores de consumos entre os produtos/ eventos.

4.10. Conclusões dos testes

Na presente secção estão apresentadas as conclusões do trabalho, após a realização dos testes que foram apresentados na secção anterior. As conclusões dos testes serão apresentadas por áreas tal como foram divididos os testes. Adicionalmente, foi atribuído um nível de criticidade a cada conclusão identificada, de modo priorizar a criticidade de cada problema. Esta classificação tem por base a matriz de risco apresentada na secção 3.1.5.

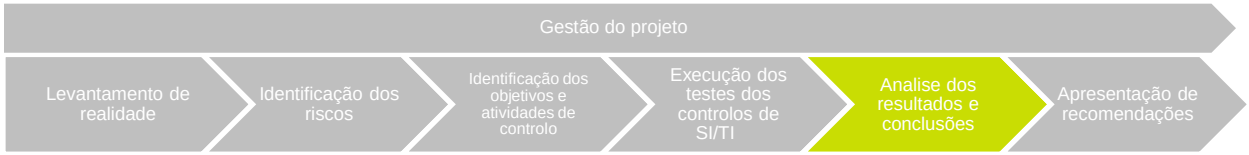

Imagem 36 - Fase conclusões dos testes

4.10.1. Geral

Através das auditorias realizadas, bem como a partir do levantamento de negócio, foram detetadas algumas vulnerabilidades na operadora, nomeadamente:

Tabela 15 - Conclusões gerais

ID	Situação identificada	Classificação
OBS.01	Forte dependência no parceiro de negócio da operadora. Todas as atividades relativas à administração do sistema *Billing* GSM e da sua manutenção (corretiva e evolutiva) são da responsabilização do parceiro de negócio da operadora.	Nível 1
OBS.02	Existência de um conjunto alargado de atividades manuais realizadas nos sistemas da empresa, que poderiam ser automatizadas de forma a evitar a ocorrência de erros/ omissões nas atividades realizadas	Nível 2

4.10.2. Integração da informação

Através da realização dos testes periódicos, foi possível detetar vulnerabilidades na integração da receita no sistema contabilístico, nomeadamente:

Tabela 16 - Conclusões integração da informação

ID	Situação identificada	Classificação
OBS.03	Não se encontram implementados procedimentos e controlos efetivos sobre as transferências/ integrações dos dados entre os sistemas, de forma a garantir a integridade e fiabilidade da informação.	Nível 2
OBS.04	Foi identificado que um dia por mês estava a ser excluído na faturação dos consumos e carregamentos.	Nível 1
OBS.05	Foram verificadas diferenças entre os dados entregues pelo parceiro de negócio e dos dados que se encontravam registados no billing.	Nível 1
OBS.06	Produtos excluídos na contabilidade, devido ao incorreto mapeamento entre as listagens de produtos entre o sistema Billing	Nível 1

	GSM e o sistema Contabilístico. – ;	
OBS.07	Não se encontram implementados controlos às rubricas contabilísticas antes da sua contabilização.	Nível 1
OBS.08	Não se encontram implementados controlos entre a informação que se encontra na interface Cobranças & Consumos log com a informação que se encontra na contabilidade.	Nível 1

Por falta de todos os controlos enumerados anteriormente, foram identificadas diferenças monetárias, entre a informação que chegou à operadora do sistema *Billing* GSM com a informação que chegou à contabilidade. Algumas causas foram já identificadas, outras serão identificadas após a auditoria aos SI/TI.

4.10.3. Gestão de operações e CPD

Tabela 17 - Conclusões gestão de operações e CPD

ID	Situação identificada	Classificação
OBS.08	Não está documentado o procedimento relativo à gestão de operações (gestão de *jobs/ batches).* Este procedimento deverá conter uma lista dos processos *job/ batch* definidos (nomeadamente os de maior criticidade), as normas e orientações relacionadas com a aprovação/ calendarização de jobs, assim como as atividades de monitorização, deteção e correção de exceções e os respetivos responsáveis.	Nível 2
OBS.09	Os *jobs/ batches* processados nos sistemas da operadora não estão a ser controlados efetivamente, tendo sido verificado que: - O acesso à criação, modificação e eliminação de *jobs/ batches* não se encontra restrita, existindo um elevado número de administradores e de utilizadores com acessos desadequados face às suas necessidades; - As alterações realizadas aos *jobs* aplicacionais definidos não são registadas/ documentadas, impossibilitando o *tracking* destas situações e o controlo/ monitorização das mesmas; - Não existe um registo das operações realizadas em log da execução dos jobs do sistema *Billing* GSM, bem como o parceiro de negócio que não reporta qualquer relatório de manutenção à operadora; e - Os *logs* de processamento dos sistemas de Cobranças e Contabilidade, são mantidos apenas durante um período de retenção de dois meses. A correção dos erros de processamento não está assegurada pela operadora.	Nível 2
OBS.10	Não se encontram definidos/ formalizados os procedimentos de *backup* implementados e aprovados na operadora, para os sistemas em âmbito. A operadora não tem controlo de monitorização/ revisão dos *backups* dos dados do sistema *Billing* GSM, estando neste particular totalmente dependente do fornecedor externo.	Nível 2

OBS.11	Verificou-se que não se encontra definido um plano de testes de *restore* periódicos às tapes de *backup*, nem é efetuado o armazenamento *off-site* das tapes	Nível 2
OBS.12	Não se encontra implementada uma estratégia de recuperação em caso de desastre (DRP – *Disaster Recovery Plan*) e continuidade de negócio (BCP – *Business Continuity Plan*).	Nível 3
OBS.13	Não estão formalmente definidos procedimentos de gestão e controlo dos acessos físicos ao CPD. Não está assegurado o controlo efetivo/ adequado dos acessos físicos ao CPD da operadora. Adicionalmente, o CPD onde se localiza o servidor do sistema *Billing* GSM, é totalmente controlado pelo parceiro de negócio, não existindo qualquer controlo de segurança realizado por parte da operadora.	Nível 2

4.10.4. Gestão de segurança da informação

Tabela 18 - Conclusões gestão de segurança de informação

ID	Situação identificada	Classificação
OBS.14	A operadora dispõe de uma política de segurança que considere os recursos, designadamente pessoas, infraestruturas, aplicações e informação. No entanto, esta política deverá ser revista de acordo com os *standars* de segurança, ISO 27K - ISO 27011 *Telecommunication*, aprovada formalmente e comunicada à organização.	Nível 3
OBS.15	Não se encontram definidos procedimentos, de classificação da informação quanto ao nível de criticidade e relevância para o negócio, ou seja, a proteção da informação não é realizada de acordo com a sua criticidade para o negócio	Nível 2
OBS.16	Não se encontram definidos procedimentos, de gestão (criação, alteração e remoção) de acessos dos utilizadores dos SI/TI, assim como não estão definidas as regras de nomenclatura a serem seguidas aquando da criação de *user-ids* nos SI/TI.	Nível 2
OBS.17	Verificámos que não se encontram formalmente definidos os procedimentos de revisão periódica dos perfis de acesso de forma a validar se estes se mantêm atualizados face à função/ responsabilidade dos colaboradores. Adicionalmente, verificámos que não são realizadas revisões periódicas aos acessos com o objetivo de identificar utilizadores genéricos, duplicados ou perfis inadequados às funções dos utilizadores.	Nível 2
OBS.18	Verificámos que não se encontram formalmente definidos procedimentos de atribuição de acessos que considerem a atribuição de acessos alargados (e.g. administrador) a nível aplicacional, do sistema operativo e bases de dados, quem deverá ter este tipo de acessos e como os mesmos são controlados/ monitorizados.	Nível 2
OBS.19	Foram identificadas exceções ao bom funcionamento do controlo de acessos dos utilizadores aos sistemas de informação. Da análise realizada aos utilizadores e parâmetros de segurança definidos nos sistemas, verificámos que:	Nível 1

A – .	- Não é mantida uma listagem dos colaboradores que atualmente trabalham na operadora; - Os acessos aos sistemas e bases de dados que se encontram atribuídos estão desajustados face às necessidades dos colaboradores. Existe um grande número de utilizadores com acessos alargados e utilizadores com designação genérica; - Os atuais mecanismos de autenticação não estão configurados de acordo com as melhores práticas e não existe um registo e monitorização de eventos relacionados com a segurança dos sistemas.	
OBS.20	A operadora não contém um modelo de continuidade de negócio que englobe um modelo de governo, equipas de suporte, planos de suporte bem como uma estratégia de sensibilização/ formação das equipas, por forma a criar uma dedicação para um processo de continuidade de negócio da empresa. Adicionalmente, não está definida uma estratégia de continuidade de negócio, não estando assegurada a recuperação dos sistemas em caso de desastre.	Nível 2
OBS.21	Não se encontra definida uma matriz de segregação de funções da operadora, que possa servir de base ao processo de atribuição/ alteração de acessos, evitando a atribuição de acessos com eventuais conflitos críticos ou garantidos que estes são conhecidos e devidamente controlados/ monitorizados.	Nível 2

4.10.5. Gestão de alterações

Tabela 19 - Conclusões gestão de alterações

ID	Situação identificada	Classificação
OBS.22	Está formalmente definido o procedimento de gestão de alterações que descreva as seguintes principais fases e responsabilidades: (i) Definição de requisitos; (ii) Análise e aprovação; (iii) Desenvolvimento; e (iv) Testes. No entanto, a gestão de alterações é registada através de uma folha de excel, sendo esta gerida por um elemento da DSI.	Nível 3
OBS.23	Não se encontram implementados procedimentos e controlos efetivos de gestão de alterações ao nível dos SI/ TI, bases de dados e sistema operativo, nomeadamente no que respeita ao envolvimento dos owners, a provisão de requisitos, acompanhamento de alterações, testes e passagem a produção. Não são mantidas de forma consistente a evidência do controlo das alterações introduzidas ao nível do SI/ TI.	Nível 1
OBS.24	Não existe um controlo efetivo por parte da operadora, das alterações realizadas pelo fornecedor externo, ao sistema Billing GSM.	Nível 1

4.11. Recomendações de melhoria/ projeto

A presente secção tem como objetivo apresentar recomendações que se implementadas, irão mitigar os riscos que têm sido estudados ao longo do presente relatório.

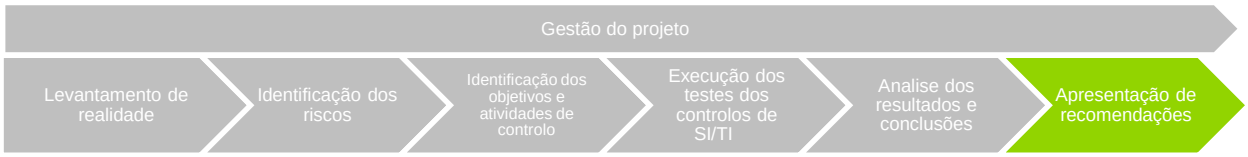

Imagem 37 - Fase apresentação de recomendações

Geral

- A operadora deve realizar um controlo de monitorização/ revisão das operações realizadas pelo parceiro de negócio. Este controlo engloba gestão dos processos de *job/ batch* execução de *backups*. Adicionalmente, a operadora deve realizar trimestralmente, uma revisão aos acessos do sistema *Billing* GSM, bem como à respetiva base de dados e sistema operativo; e
- Reavaliar as atividades que se encontram a ser executadas nos sistemas da operadora, manualmente de forma a evitar a ocorrências de erros/ omissões das atividades realizadas.

Integração da informação

- Reavaliar o processo de faturação dos processos de consumos e carregamentos dos números pré-pagos da rede GSM, por forma a considerar todos os dias do mês;
- Realizar mensalmente os testes periódicos que foram passados pela Deloitte à equipa de receita e faturação, onde proporciona à operadora um controlo, nomeadamente a:
    - Análise da integridade da informação que foi fornecida pelo parceiro de negócio;
    - Análise dos produtos, a partir de uma reconciliação das listagens dos produtos fornecidos pelo parceiro de negócio e os produtos que definidos na contabilidade;
    - Análise aos dados dos consumos e carregamento de saldo dos números pré-pagos GSM carregados na interface Cobranças & Consumos; e
    - Análise aos dados de consumos e carregamentos de saldos em números pré-pagos GSM estão devidamente refletidos nas rubricas contabilísticas.

A operadora já se encontra a realizar todas as recomendações anteriormente descritas. A equipa da Deloitte já realizou ações de formação, onde realizou uma "passagem de pastas" dos testes periódicos à equipa de receita e faturação da operadora, estando sempre disponível para esclarecimento de dúvidas sempre que necessário.

Gestão de operações

- Devem ser formalmente definidos os procedimentos de gestão de operações a serem seguidos pelos colaboradores, nomeadamente os processos *job/ batch* definidos (nomeadamente os de maior criticidade), as normas e orientações relacionadas com a aprovação/ calendarização de jobs, assim como os procedimentos e responsáveis pela sua monitorização e correção;

- Formalizar os procedimentos de gestão de *backups*, os quais deverão incluir, entre outros, os seguintes aspetos:
  - os sistemas, aplicações e dados abrangidos pelo *backup* e respetivas periodicidades de execução e períodos de retenção de acordo com análise da criticidade da informação;
  - definição de responsabilidades pelas tarefas relacionadas com *backups* (e.g. realização, monitorização);
  - plano de rotação e fluxo de dados de *backup* (*on-site*, *off-site*, *recovery site*);
  - processo de criação, catalogação e inventariação de *tapes*;
  - processo de eliminação de informação após período de retenção;
  - processo de registo do transporte e arquivo de tapes de *backup*; e
  - procedimentos de monitorização/ acompanhamento de alterações nas leis e regulamentações que afetem os períodos de retenção de dados.

- Definir e formalizar um DRP e um BCP que inclua todas as áreas críticas da operadora, nomeadamente sistemas em âmbito (Billing GSM, Cobranças e Contabilidade), de forma a assegurar a continuidade das operações em caso de ocorrência de um incidente de grande impacto;
- Definir/ documentar um procedimento de gestão/ revisão de acessos físicos ao CPD, às áreas reservadas e técnicas e aos edifícios, e adotar controlos de monitorização adequados;
- Reavaliar os controlos físicos e ambientais ao CPD. Adoção de medidas corretivas ou de salvaguarda para algumas vulnerabilidades identificadas permitirão assegurar uma maior fiabilidade da segurança em torno do CPD, tais como:
  - Implementação de ar-condicionado redundante e sistema de monitorização de humidade;
  - Instalação de mecanismos automáticos de extinção de incêndios;
  - Implementação de uma saída de emergência (as portas do CPD devem abrir para o seu exterior e possuir barras de saída rápida);
  - Manutenção periódica dos extintores de incêndio existentes. Instalação de extintores manuais dentro do CPD;
  - Permitir a fácil identificação e acesso aos extintores existentes;
  - Remoção de todo o material inflamável existente nas instalações do centro de processamento de dados;

- Instalação de sinalização no interior do centro de processamento de dados relativamente à proibição de fumar, comer e beber;
- Realização de manutenções periódicas aos UPS, para verificar o seu correto funcionamento; e
- Implementação de mecanismos de monitorização por meio de circuito interno de vídeo.

Gestão de sistemas de informação

- Implementar práticas de segurança da informação normalizadas (e.g. ISO/IEC 27001 que se encontra descrita na secção 3.1.2);
- Desenvolvimento de um procedimento de gestão e revisão de acessos a todos os sistemas/ aplicações e rede da operadora, que inclua a definição de regras a adotar para a nomenclatura dos utilizadores;
- Implementar uma listagem interna, com os colaboradores que trabalham atualmente na operadora;
- Definição da matriz de segregação de funções, controlos e responsabilidades;
- Avaliação dos controlos de segregação de funções (e.g. acessos, *reporting*, manuais);
- Clarificação/ definição dos perfis funcionais de acesso (em estreita colaboração com as respetivas áreas de negócio);
- Analisar em detalhe os perfis de acesso e acessos atribuídos ao nível dos sistemas;
- Deverá ser assegurada a adequada documentação do pedido e respetiva aprovação do acesso aos sistemas de informação, permitindo assim a validação efetiva do processo de atribuição de acessos implementado;
- Avaliar a relevância da existência dos utilizadores genéricos, e se possível criar utilizadores unívocos, permitindo assim identificar o colaborador responsável pelas ações realizadas em sistema. Manter uma lista atualizada dos utilizadores genéricos autorizados que, deverá conter a identificação do responsável pelo utilizador, assim como a justificação para a sua manutenção; e
- Avaliar a pertinência das permissões alargadas existentes ao nível dos sistemas e subsequente remoção dos acessos desnecessários atribuindo em alternativa as permissões mínimas necessárias para o desempenho das funções dos respetivos colaboradores.
- Modificar os parâmetros de segurança dos sistemas de modo a:
  - Definir com 6 ou mais carateres o tamanho mínimo da *password*;
  - Definir um período de 30 a 90 dias, de validade da password;
  - Implementar a validação do histórico das ultimas *passwords* (6 ou mais);
  - Obrigar a que o número de caracteres diferentes entre a nova e a ultima *password*, seja de, pelo menos, 5 caracteres;
  - Definir como máximo de 3 tentativas, a quantidade de vezes que o utilizador pode introduzir *passwords* erradas antes que esta seja automaticamente bloqueada;

    - Terminar a sessão do utilizador por excesso de inatividade (max. 1800 segundos);
    - Impedir a abertura de múltiplas sessões para o mesmo *userID*.
- Implementação de um manual de segurança do utilizador, onde englobe os seguintes componentes:
    - Identificação áreas de *compliance*.
    - Apresentar os riscos associados aos comportamentos dos utilizadores para com os sistemas; e
    - Apresentar as regras de segurança a serem adotadas de acordo com as melhores práticas.

Gestão de alterações

- Embora exista uma descrição de alto nível do fluxo do processo de gestão de alterações, este processo deverá ser detalhado de forma a que sejam documentadas todas as exceções (i.e. diferença entre os procedimentos de alterações evolutivas e corretivas), sejam definidos *templates* para a descrição das alterações (pedido) e respetivas aprovações, planeamento dos testes de aceitação, aprovação dos testes de aceitação e aprovação para a entrada em produtivo;
- Definição de plano de testes e envolvimentos das áreas funcionais (*owners*);
- Avaliar a adoção de ambientes de testes e qualidade, para as alterações realizadas aos sistemas, bases de dados e sistema operativo; e
- Desenvolver um controlo por parte da operadora, relativamente à implementação de um sistema de controlo e registos das alterações efetuadas aos sistemas, bases de dados e sistema operativo. Contendo os seguintes registos: aprovação da alteração antes da implementação; planeamento testes de aceitação realizados, aprovação dos testes de aceitação e aprovação para entrada em produção.

5. Conclusão

O presente trabalho desenvolveu-se com foco num objetivo, ajudar a garantir a correta captação da receita da operadora.

Este objetivo foi, numa fase inicial, a realização de um estudo sobre a operadora e respetivo ciclo de receita, e identificar com base nesse conhecimento os riscos com impacto na receita da operadora. Como a operadora não continha os seus processos de negócio devidamente documentados, o que impossibilitava realizar um planeamento e avaliação do ciclo de receita, foi realizado o levantamento dos processos de negócio da operadora com impacto na receita. Para efetuar o levantamento dos processos de negócio da operadora com impacto na receita, foi necessário proceder a várias reuniões com os diversos departamentos, por forma a entender, analisar e documentar. Após a conclusão da documentação, foi necessário reunir novamente com os departamentos da operadora, para validar que toda a informação se encontrava devidamente documentada. Aquando da conclusão da documentação dos processos de negócio da operadora, foram identificados através do RIM e de uma matriz de risco realizada pela Deloitte na última passagem pela operadora, os riscos com impacto na receita da operadora.

Simultaneamente, foram realizados testes aos consumos e carregamentos de modo a identificar perdas na integração da receita nos SI/ TI. A partir dos testes realizados, foram identificadas falhas graves na integração da informação dos SI/ TI dos carregamentos e consumos potenciando perdas na receita da operadora. Estes testes foram passados à equipa de receita e faturação da operadora, de forma a criar uma ferramenta de controlo, ajudando assim a operadora a controlar a receita destes dois processos.

Na segunda fase do trabalho, foi decidido em conselho de administração da operadora, que seria necessário mitigar em primeiro lugar os riscos associados aos SI/ TI do processo de faturação. Esta decisão teve como base as falhas nos processos de carregamentos e consumos identificados nos testes anteriormente referenciados. De forma a mitigar os riscos associados aso SI/ TI do processo de faturação, foi decidido que seria necessário realizar uma CGI.

A CGI iniciou-se com reuniões com a operadora de forma a entender a organização e os controlos aos SI/ TI pois só assim foi possível reavaliar os riscos dos SI/ TI e completá-los de forma a adaptá-los à realidade da operadora. Após esta definição foi necessário identificar os objetivos de controlo e atividades de controlo, a fim de mitigar os riscos anteriormente referenciados. Este processo teve como auxilio o RACK na identificação dos objetivos e atividades de controlo. Estando as atividades identificadas foi necessário desenhar testes para garantir que as estas eram devidamente realizadas. Com os testes desenhados, foi criada uma listagem de pedidos de informação para solicitar à operadora, mais concretamente à DSI.

Ao longo do trabalho existiram dificuldades na disponibilização da informação, tendo sido necessária a intervenção por parte dos elementos de topo da equipa da Deloitte e da operadora, para que a informação fosse disponibilizada. Contudo, a mesma não foi entregue nos prazos estipulados. Muita informação solicitada não foi disponibilizada ou não existe, o que impossibilitou a realização de alguns testes. Nestas situações, o teste em questão ficou inefetivo, não existindo a possibilidade de garantir que a atividade de controlo fosse devidamente realizada.

No final dos testes realizados foram detetadas várias vulnerabilidades ao nível da segurança dos SI/ TI. Por isso foi criada uma listagem de oportunidades de melhoria para serem implementadas no futuro que vão mitigar muitos riscos e levar a um correto e completo controlo dos SI/ TI, para garantir uma correta captação da receita.

A realização do estágio em auditoria em SI/ TI, mostrou-me que existia uma vertente diferente à que é lecionada na vida académica. Aprendi que os SI/ TI necessitam de ser controlados e testados periodicamente pois uma empresa que não tem controlo nos seus SI/ TI corre grandes riscos que podem levar a perdas significativas na receita, colocando assim em risco, a própria vida da empresa.

Bibliografia

[1] techopedia. [Online]. Available: https://www.techopedia.com/definition/28727/batch-job-sap.

[2] "SOX," 2013. [Online]. Available: http://www.sec.gov/about/laws.shtml#sox2002.

[3] "ISO 22301," *Societal security — Business continuity,* 2012.

[4] "ISO 22301," 2013. [Online]. Available: http://pecb.org/iso22301/.

[5] ITIL - Service operation processes, 2011.

[6] U. C. d. G. d. S. d. Informação, THE IT INFRASTRUCTURE LIBRARY (ITIL).

[7] A. Serafim, "Portal Gestão," [Online]. Available: http://www.portal-gestao.com/item/6955-matriz-de-eisenhower-como-trabalhar-de-maneira-mais-eficiente.html.

[8] ACL Services Ltd., "ACL - Getting Started," 2006.

[9] "ACL," ACL, [Online]. Available: http://docs.acl.com/acl/920/index.jsp?topic=%2Fcom.acl.user_guide.help%2Fdata_analysis%2Fc_about_sorting.html.

[10] K. v. H. T. d. J. C. Wil van der Aalst, Gestão de Workflows. Modelos, métodos e sistemas, Setembro 2009.

[11] Cymo, "BPMN 2.0 - Notação para Modelagem de Processos de Negócio".

[12] Governance Institute, "CobIT 4.1 Excerpt".

[13] National Center of Security and Protection, [Online]. Available: http://www.natsp.org/Risk%20Mgmt%20&%20Analysis.html.

[14] U. o. Delaware, "University of Delaware - Finance," [Online]. Available: http://www.udel.edu/Treasurer/intcntrldef.html.

[15] Deloitte, "Risk Intelligence Map Usage Guide," Deloitte, 2011.

[16] CGE, "CGE," [Online]. Available: http://www.cgerisk.com/knowledge-base/risk-assessment/risk-matrices.

[17] R. R. Moeller, COSO - Enterprise Risk Management, New Jersey: John Wiley & Sons, Inc., 2007.

[18] A. Carneiro, Auditoria de sistemas de informação, 2001.

[19] Symantec, "http://www.symantec.com/information-protection/," 2015. [Online].

[20] w. N. community, "Nagios," Agosto 2015. [Online].

Anexos

Anexo 1 – Riscos do projeto

Descrição do risco do projeto	Mitigação do risco dependente de Deloitte	Mitigação do risco dependente da operadora
Gestão do Projeto		
É importante garantir a constante qualidade do projeto	Planear e priorizar atempadamente todas as atividades do projeto	Validar atempadamente (dentro do *timing* e no formato acordados) os *outputs* de cada atividade
É importante garantir uma correta manutenção do âmbito, calendário e atribuição das responsabilidades do projeto	Alertar relativamente a impactos qualitativos, quantitativos e temporais associados a alterações ao âmbito do projeto; Cumprir os prazos acordados, face ao tempo previsto de duração do projeto; e Cumprir as responsabilidades acordadas no âmbito das equipas de projeto.	Manter o âmbito referido na proposta; Não proceder à alteração dos pressupostos e âmbito do projeto; Participar ativamente e regularmente nas reuniões de ponto de situação; e Cumprir as responsabilidades acordadas no âmbito das equipas de projeto.
É importante conhecer a ocorrência de alterações aos procedimentos ou políticas na empresa	Solicitar a comunicação de todas as alterações que ocorrem dentro da empresa, com impacto no projeto	Comunicar à equipa de projeto qualquer alteração que ocorra na empresa, com impacto no projeto
É importante garantir a confidencialidade da informação	Garantir a confidencialidade da informação recebida e utilizá-la exclusivamente para fins do projeto	Facultar acesso a toda a informação relevante para a execução do projeto
É importante garantir que existe comunicação entre os diversos departamentos da operadora.	Manter uma comunicação clara e efetiva dentro e fora da empresa, de modo a colmatar as falhas de comunicação	Clarificar a importância da necessidade de comunicação entre os diversos departamentos da operadora, incluindo da parte de terceiros afetos à operadora (e.g. fornecedores externos).
É importante garantir a disponibilização da informação e a disponibilidade do cliente para reunir, de forma atempada	Alertar a operadora para a necessidade de realização de pontos de situação periódicos; e Comunicar à operadora a informação necessária para a realização do projeto, bem como os prazos para entrega da mesma.	Disponibilizar a informação necessária para a realização do projeto, nos *timings* definidos e no formato acordado, quer da operadora quer de prestadores de serviços (e.g. fornecedores externos).
É importante garantir a disponibilidade de recursos	Afetar recursos conforme preconizado ao longo da presente proposta; e Assegurar disponibilidade destes recursos para participar nas sessões de trabalho e reuniões, conforme planeado e acordado.	Afetar recursos conforme preconizado ao longo da presente proposta; e Assegurar disponibilidade destes recursos para participar nas sessões de trabalho e reuniões, conforme planeado e acordado.
Gestão das Expectativas		
É importante garantir que existe alinhamento de todas as pessoas envolvidas no projeto relativamente ao objetivo do mesmo	No *kickoff*(reunião de inicio do projeto, onde são apresentados os objetivos, calendarização, entre outros), garantir que os objetivos do projeto são compreendidos e aprovados por parte da operadora.	Aprovar os objetivos do projeto e garantir a sua compreensão às pessoas relevantes na operadoras Disponibilidade durante o projeto, sempre que necessário

É importante garantir um *sponsorship* adequado	Realizar todas as atividades corretamente, de acordo com o planeamento definido	Reunir periodicamente com a equipa de projeto para avaliar o cumprimento de todos os objetivos do projeto, de acordo com o planeamento
Equipa		
É importante garantir a boa comunicação entre os elementos da equipa	Comunicar com os elementos da equipa a todo o momento, de modo a evitar constrangimentos que possam ter impacto no planeamento do projeto Manter os elementos *seniors* da equipa sempre atualizados relativamente às atividades em curso e reportar os constrangimentos sempre que ocorram (e.g. ausência de elemento da equipa por motivos de doença)	n.a.
É importante conhecer o papel dos interlocutores	Garantir o conhecimento do papel dos interlocutores, nomeadamente através de reuniões de confirmação com a operadora.	Facultar toda a informação necessária para que a equipa de projeto detenha o conhecimento do papel dos interlocutores da operadora.
É importante garantir que toda a equipa tem conhecimento das tecnologias e metodologias do projeto	Para conhecimento à equipa, de forma que a mesma se encontre devidamente familiarizada com as tecnologias e metodologias utilizados no projeto	n.a.
Logística		
É importante garantir que se mantém toda a informação do projeto, ou seja, que não ocorrem perdas de informação (e.g. por quebra de energia)	Utilizar pontos de rede para energia alternativa.	Garantir a existência de UPS, geradores de energia alternativos.
É importante garantir que existem equipamentos para a realização do trabalho	Planear todo o material necessário para a realização do projeto; Manter atualizados os*backups*da informação do projeto, de modo a evitar constrangimentos no caso de, por exemplo, *crash* de computadores e falhas de ligação à internet.	Manter atualizados os *backups* de informação relevante.
É importante garantir a disponibilização de espaço físico para a realização do projeto, nomeadamente sala para trabalho e/ou reuniões	Comunicar, à operadora, a necessidade da disponibilização de espaço, tendo em conta os recursos da equipa	Disponibilizar espaços físicos necessários à realização do projeto
É importante garantir a disponibilização de wc's	Verificar a disponibilização de wc's e, em caso de constrangimento, comunicar à operadora	Disponibilizar wc's
É importante garantir a disponibilização de meios de acesso aos edifícios	Comunicar, à operadora, a necessidade da disponibilização de acessos ao edifício a todos os elementos da equipa	Disponibilizar acesso aos edifícios

É importante garantir a existência de meios para partilha de informação (e.g. grandes volumes de dados)	Alertar o cliente para a necessidade de existência de meios para partilhada de informação com grande volume de dados	Disponibilizar meios para a partilha de informação com grande volume de dados (e.g. pasta de rede partilhada)
Validação		
É importante garantir a qualidade do trabalho realizado	Realizar pontos de situação periódicos de equipa; e Assegurar a existência de revisões do trabalho (e.g. por parte dos elementos *seniors*).	Realizar pontos de situação periódicos com a equipa de projeto.
É importante garantir a comunicação das conclusões finais do projeto e consequente celeridade na aprovação	Preparar documentos de suporte ao trabalho efetuado no decorrer do projeto.	Assumir todas as decisões na implementação do projeto; e Estar presente na apresentação das conclusões finais do projeto, analisar as mesmas e confirmar a respetiva aceitação atempada.

Anexo 2 – Riscos

ID	Tipo de Risco	Fatores de risco	Fonte	Descrição dos fatores de risco
FR.01	Supervisão de risco	Supervisão inadequada das atividades de gestão de risco	*Risk Map*	- Consiste na falta de validação, monitorização e controlo das atividades de gestão de risco; - Tendo como consequência a não identificação do risco e respectivos objetivos de controlo, bem como as atividades que mitiguem o mesmo; e - Potenciando a não obtenção dos resultados esperados.
FR.02	Fraude externa	Fraude por parte do fornecedor ou parceiro	*Risk Map*	- Consiste na existência de esquemas ilícitos, envolvendo o engano deliberado, de forma a prejudicar a empresa para obter ganhos pessoais por parte de fornecedores; - Podendo implicar a perda/ adulteração de informação e a perda de confidencialidade, pondo em causa a segurança da empresa e a sua imagem pública; e - Conduzindo a uma prestação de serviço ao cliente de menor qualidade e consequente perda de receita.
FR.03	Perigos/ perdas catastróficas	Situações epidémicas (e.g. malária, ébola)	*Risk Map*	- Consiste em doenças de origem infeciosa, cuja incidência, pode aumentar consideravelmente, sendo a sua ocorrência um processo dinâmico, que resulta de uma sequência de eventos (e.g. introdução de um novo agente patogénico); - Tendo como consequência a afetação direta dos recursos humanos da empresa, podendo tornar-se de alta gravidade, sem que a empresa possa ter controlo sobre a mesma; e - Conduzindo à perda de recursos e consequente incumprimento de prazos de entregas ou de não obtenção dos resultados esperados.

FR.04	Perigos/ perdas catastróficas	Desastres naturais	*Risk Map*	- Consiste na ocorrência de um evento físico (e.g. sismo, furação, terramotos), no qual não existe intervenção humana; - Tendo como consequência danos à empresa, diretos ou indiretos (e.g. destruição de edifícios, doença, morte); e - Podendo conduzir à perda total ou parcial de informação e/ ou das instalações da empresa, nomeadamente à falta de recursos para a realização das atividades da empresa.
FR.05	Perigos/ perdas catastróficas	Terrorismo/ ações causadas pelo Homem	*Risk Map*	- Consiste na utilização de violência, física e/ ou psicológica, através de ataques localizados a pessoas e/ ou instalações; - Tendo como consequência danos à empresa e/ ou colaboradores, diretos ou indiretos (e.g. destruição de edifícios, incêndios, inundações, doença, morte, pânico entre a população); e - Podendo conduzir à perda total ou parcial de informação e/ ou das instalações da empresa, nomeadamente à falta de recursos para a realização das atividades da empresa.
FR.06	Requisitos de terceiros/ *join venture*	Risco contractual	*Risk Map*	- Consiste na probabilidade de perda decorrente de falha na execução de contractos; - Tendo como consequência atrasos no cumprimento do planeamento, disponibilização de informação e/ ou na entrega do *output* do produto/ serviço; e - Conduzindo à perda de receita devido ao incumprimento das clausulas contratuais.
FR.07	Concentração de negócio	Excesso de dependência num fornecedor	*Risk Map*	- Consiste na dependência da empresa relativamente a produtos fornecidos/ serviços prestados por um único fornecedor; - Tendo como consequência o fraco ou inexistente poder de negociação da empresa perante o fornecedor; e - Podendo conduzir ao fracasso das atividades dependentes desse fornecedor e ao incumprimento dos respectivos prazos, comprometendo o negócio da empresa.
FR.08	*Outsourcing*	Perda de competências *core*	*Risk Map*	- Consiste na carência de competências cruciais para exercer as atividades da empresa; - Tendo como consequências a falta de capacidade para realização com sucesso dos projetos desenvolvidos e a fraca qualidade dos mesmos; e - Podendo conduzir à falha no bom funcionamento do negócio da empresa e respetiva prestação de serviços ao cliente.
FR.09	*Outsourcing*	Dependência numa única fonte de funções *core* prestadas por terceiros	*Risk Map*	- Consiste na dependência de uma única fonte de recursos externos para o desenvolvimento de funções *core* da empresa; - Tendo como consequências a fraca proteção do *know-how* (e.g. metodologias, processos) e o fraco ou inexistente poder de negociação da empresa perante o fornecedor; e - Conduzindo ao não desenvolvimento interno de competências para funções *core*, dependendo de recursos externos para a resolução de problemas nas mesmas.

FR.10	*Outsourcing*	Falha na satisfação de requisitos por parte da empresa de *outsourcing*	*Risk Map*	- Consiste na incapacidade de responder às necessidades de negócio, por parte da empresa de *outsourcing*; - Tendo como consequência a fraca qualidade dos serviços prestados, podendo ter impacto no cumprimento de prazos e na entrega de *outputs* do projeto; e - Podendo conduzir à não obtenção dos resultados esperados e ao término do relacionamento com a empresa de *outsourcing*.
FR.11	*Outsourcing*	Falha na revisão jurídica de contracto de *outsourcing*	*Risk Map*	- Consiste na ausência de revisões aos termos dos contractos com empresas de *outsourcing*; - Tendo como consequências a falta de salvaguarda de alterações de âmbito (situações que possam prejudicar a empresa), e dos níveis de serviço prestados por terceiros e subsequentemente ao serviço prestado aos clientes contemplados nos contractos; e - Podendo conduzir à falta de conformidade com a legislação atual existente.
FR.12	Atribuição de preços	Produtos/ serviços com preços inadequados	*Risk Map*	- Consiste na definição incorreta de preços de produtos/ serviços, por não se ter em conta os custos totais de produção e a margem dos ganhos por produto/ serviço; - Tendo como consequências a fuga de clientes que, por falta de competitividade de preços, vão à concorrência (overcharging) e/ ou perda de receita, caso os produtos vendidos/ serviços prestados tenham um preço muito abaixo do esperado (undercharging); e - Podendo conduzir a processos de insolvência/ falência por insustentabilidade do negócio.
FR.13	Atribuição de preços	Pouca flexibilidade no mecanismo de atribuição de preços	*Risk Map*	- Consiste na falta de adaptação do mecanismo de definição de preços; - Tendo como consequência a impossibilidade de alteração da tabela de preços em resposta aos eventos económicos (e.g. recessão económica, depressão económica); e - Conduzindo a perda de receita e à perda de clientes.
FR.14	Atribuição de preços	Estratégia de preços internacional ineficaz	*Risk Map*	- Consiste na falha na estratégia no estabelecimento de preços de produtos/ serviços fora do mercado nacional; - Tendo como consequência a fraca capacidade de competitividade em mercados internacionais e subsequente redução de vendas, quer devido à falta de conhecimento quer da incapacidade de produção/ distribuição/ *marketing* dos produtos/ serviços para este tipo de mercado; e - Conduzindo à perda de receita da empresa.
FR.15	Segurança pessoal	Segurança pessoal inadequada	*Risk Map*	- Consiste na falta de proteção dos colaboradores, devido ao incumprimento da implementação da política de segurança no trabalho; - Tendo como consequências o aumento da probabilidade de acidentes e/ ou doenças ocupacionais, a desmotivação e desinteresse dos colaboradores e a perda de colaboradores devido aos acidentes; e - Podendo conduzir à perda de eficiência por parte dos colaboradores e/ ou perda financeira devido a multas em caso de negligência.

FR.16	Segurança física	Falha na implementação dos controlos de segurança	*Risk Map*	- Consiste na incorreta implementação dos controlos de segurança física (e.g. segurança ou rececionista, fechaduras ou chaves, cartões de acesso); - Tendo como consequências o acesso ilícito às infraestruturas, edifícios, equipamentos, materiais ou documentação e/ ou a apropriação indevida dos mesmos; e - Conduzindo à perda/ fuga de informação e/ ou equipamento da empresa.
FR.17	Segurança física	Falha nas políticas e processos de segurança dos ativos físicos	*Risk Map*	- Consiste na incapacidade de definir políticas e processos que garantam a segurança dos ativos físicos; - Tendo como consequências a implementação de controlos de segurança que não impedem o acesso ilícito às infraestruturas, edifícios, equipamentos, materiais ou documentação e/ ou a apropriação indevida dos mesmos; e - Conduzindo à perda/ fuga de informação e/ ou equipamento da empresa.
FR.18	Segurança física	Planos de mitigação de riscos de segurança física ineficazes	*Risk Map*	- Consiste na falta de planos de mitigação de riscos de segurança física que sejam capazes de atingir os objetivos pretendidos; - Tendo como consequência o acesso indevido às infraestruturas e instalações da empresa, bem como à informação crítica e subsequente divulgação e quebra de confidencialidade da mesma; e - Podendo conduzir à quebra de relacionamento com os clientes e consequente perda de receita.
FR.19	Segurança física	Roubo de ativos	*Risk Map*	- Consiste na apropriação indevida de ativos, por meios enganosos; - Tendo como consequência a impossibilidade de executar tarefas para as quais esses ativos sejam necessários; e - Conduzindo à perda de informação, bem como ao prejuízo monetário associado aos ativos.
FR.20	Gestão de processos	Incapacidade de monitorizar ativos e informação relacionada	*Risk Map*	- Consiste na incapacidade de monitorizar os ativos e informação relacionada; - Tendo como consequência a perda parcial/ total dos ativos e da informação relacionada, em caso de roubo/ perda dos mesmos; e - Conduzindo à perda de informação e perda de receita.
FR.21	Gestão de processos	Processos lógicos inadequados	*Risk Map*	- Consiste na utilização de fluxos lógicos não adequados à gestão de processos da empresa; - Tendo como consequências o incorreto encadeamento das atividades dos processos e a subsequente incorreta implementação e execução dos processos da empresa; - Podendo conduzir à ineficácia dos processos e à perda de receita.
FR.22	Gestão de processos	Processos de negócio inefetivos/ ineficazes	*Risk Map*	- Consiste na inexistência de processos de negócio eficazes/ efetivos; - Tendo como consequência a incapacidade de atingir os objetivos definidos da empresa e de mitigar as necessidades do cliente; e - Conduzindo à perda de receita e ao fraco/ nulo crescimento da empresa.
FR.23	Utilização	Planeamento de produção inadequado	*Risk Map*	- Consiste na inexistência de planeamento adequado relativo aos processos de produção; - Tendo como consequência a falta de otimização de recursos (e.g. subaproveitamento dos recursos, pessoas, equipamentos) e a subsequente ineficácia e ineficiência dos processos de produção; e - Conduzindo à não otimização de toda a receita possível de ser gerada.

FR.24	Contabilidade	Políticas de contabilidade inapropriadas	*Risk Map*	- Consiste na inexistência de políticas de contabilidade adequadas face ao mercado em que a empresa se insere; - Tendo como consequência a impossibilidade de definir procedimentos, incluindo abordagens/ métodos de contabilidade; e - Podendo originar *reporting* financeiro que não reflete a realidade e a posição financeira da empresa, pondo em causa a viabilidade de qualquer tipo de decisões estratégicas, administrativas e organizacionais, devido à falta de atualização de políticas de contabilidade ou incorreta interpretação das normas das mesmas.
FR.25	Contabilidade	Controlo insuficiente sobre lançamentos contabilísticos	*Risk Map*	- Consiste na falta de controlo sobre lançamentos contabilísticos; - Tendo como consequência a falta de integridade da informação contabilística, não refletindo a realidade e a posição financeira da empresa; - Potenciando a existência de fraude contabilística e pondo em causa a viabilidade de qualquer tipo de decisões estratégicas, administrativas e organizacionais, devido à falta de controlo sobre os lançamentos contabilísticos da empresa.
FR.26	Contabilidade	Falta de integridade da informação financeira	*Risk Map*	- Consiste na inexistência de garantia de que a informação financeira não foi alterada de forma não autorizada ou indevida; - Tendo como consequência a perda de eficácia e confiabilidade da informação, tornando vulneráveis decisões que a partir dela são tomadas, e tirando a credibilidade da fonte que a forneceu; e - Podendo causar perdas financeiras ou outros danos (e.g. fraude na apresentação de resultados financeiros, atos de suborno, influência ilegal ou outras ações para benefício da empresa).
FR.27	Contabilidade	Falta de conhecimento das práticas e princípios de contabilidade	*Risk Map*	- Consiste na inexistência de conhecimento das práticas e princípios de contabilidade estabelecidos na empresa; - Tendo como consequência a inexistência de garantia da realização das atividades definidas de acordo com os objetivos estabelecidos; e - Conduzindo à não obtenção dos resultados esperados.
FR.28	Contabilidade	Programas e controlos de fraude insuficientes	*Risk Map*	- Consiste na falta de programas e controlos realizados para deteção da fraude; - Tendo como consequência a perda monetária para a empresa e o tempo gasto para a deteção/ mitigação da fraude; e - Podendo conduzir à perda de reputação da empresa e à perda de receita, devido à quebra nos relacionamentos com clientes.
FR.29	Gestão de Continuidade de Negócio	Incapacidade de recuperação de dados	*Risk Map*	- Consiste na falta de capacidade para recuperar dados; - Tendo como consequência a perda irreversível de informação sensível e importante; e - Conduzindo a perdas/ ruturas de processos críticos corporativos.
FR.30	Gestão de Alterações	Processos de controlo de alterações ineficazes	*Risk Map*	- Consiste na falta de processos de controlo de alterações eficazes; - Tendo como consequência a implementação de alterações duplicadas, desajustadas ou desviadas do objetivo; e - Conduzindo à obtenção de alterações nos sistemas de informação que não produzem os resultados

				esperados.
FR.31	Gestão de Alterações	Alterações não autorizadas no ambiente de produção	*Risk Map*	- Consiste na falta de controlo de realização de alterações em ambiente de produção; - Potenciando a existência de alterações por pessoas não autorizadas no ambiente de produção dos sistemas de informação da empresa; e - Conduzindo ao desvio dos resultados esperados.
FR.32	Gestão de Alterações	Realização de testes insuficientes antes da implementação	*Risk Map*	- Consiste na falta de realização de testes antes da implementação em ambiente de produção; - Tendo como consequência a implementação de alterações que não vão de encontro aos requisitos definidos; e - Conduzindo à não adequação dos sistemas de informação da empresa e, subsequente, incapacidade para obtenção dos resultados esperados.
FR.33	Gestão de Alterações	Não execução de verificação após a validação	*Risk Map*	- Consiste na falta de execução de testes de verificação da alteração após implementação; - Tendo como consequência a existência de alterações que não vão de encontro aos requisitos definidos; e - Conduzindo à não adequação dos sistemas de informação da empresa e, subsequente, incapacidade para obtenção dos resultados esperados.
FR.34	Contratação e *Outsourcing*	Licitação inadequada e seleção, contratação e continuidade de *due diligence*	*Risk Map*	- Consiste na falta de conhecimento da realidade da entidade contratada; - Tendo como consequência a aquisição de produtos/ serviços que não vão colmatar as necessidades da empresa; e - Conduzindo à não disponibilização dos resultados pretendidos.
FR.35	Contratação e *Outsourcing*	Fraca segurança e controlos de privacidade de dados de terceiros	*Risk Map*	- Consiste na incapacidade de controlar a privacidade da informação de terceiros (e.g. clientes); - Tendo como consequência a fuga de informação confidencial; e - Conduzindo a impactos negativos nos resultados da empresa e prejudicando a imagem pública da mesma.
FR.36	Segurança de Informação	Controlos de acesso ineficientes/ ineficazes	*Risk Map*	- Consiste na ineficiência/ ineficácia dos controlos de acesso lógicos; - Tendo como consequência o acesso não autorizado aos sistemas; e - Podendo conduzir à falta de integridade e confidencialidade da informação.
FR.37	Segurança de Informação	Vulnerabilidade a ataques maliciosos	*Risk Map*	- Consiste na incapacidade de impedir ataques maliciosos aos sistemas de informação da empresa; - Tendo como consequência a adulteração/ eliminação de informação do sistema com a introdução de *software* malicioso nos sistemas de informação; e - Podendo conduzir à falta de integridade e confidencialidade da informação.
FR.38	Segurança de Informação	Estratégia de antivírus ineficaz	*Risk Map*	- Consiste na falta de uma estratégia de antivírus eficaz; - Tendo como consequência a incapacidade de proteger os sistemas de informação da empresa contra vírus; e - Podendo conduzir à falta de integridade e confidencialidade da informação.

FR.39	Segurança de Informação	Aplicação prematura de *patches* de segurança	*Risk Map*	- Consiste na aplicação *patches* de segurança que não estão totalmente completos; - Tendo como consequência a abertura de falhas no sistema e consequente possibilidade de entrada a *software* malicioso; e - Podendo conduzir à falta de integridade e confidencialidade da informação.
FR.40	Segurança de Informação	Falta de segurança física/ lógica	*Risk Map*	- Consiste na falta de segurança física/ lógica da infraestrutura tecnológica; - Tendo como consequência a falta de proteção da informação e dos próprios sistemas (*hardware* e *software*); e - Podendo conduzir ao mau funcionamento do equipamento e à falta de integridade e confidencialidade da informação.
FR.41	Segurança de Informação	Falta de segregação de funções	*Risk Map*	- Consiste na inexistência de uma correta segregação de funções; - Tendo como consequência falhas na separação das responsabilidades pela execução de atividades que deverão ser realizadas por colaboradores distintos; e - Podendo conduzir a casos de fraude/ corrupção nos processos de negócio da empresa.
FR.42	Operações	Falha em garantir um agendamento e conclusão atempada dos processos	*Risk Map*	- Consiste na incapacidade em garantir um agendamento e conclusão atempada dos processos; - Tendo como consequência o incumprimento de prazos de agendamento e conclusão dos processos; e - Podendo conduzir a falhas na sequência de operação dos processos e à falta de alinhamento com as expectativas do cliente.
FR.43	Operações	Processos e ferramentas ineficientes para retenção de dados	*Risk Map*	- Consiste na falta de processos e ferramentas para realizar uma correta e completa retenção de dados; - Tendo como consequência a perda de informação e a impossibilidade de recuperação da mesma; e - Podendo conduzir a perdas, fugas e falta de integridade de informação.
FR.44	Operações	Falha em arquivar dados críticos para localizações *off-site*	*Risk Map*	- Consiste na incapacidade de arquivar dados críticos em localizações *off-site*; - Tendo como consequência a falta de segurança de informação crítica; e - Podendo conduzir a perda total/ parcial da informação em caso de problemas nos sistemas de *backups*.
FR.45	Operações	Falha em assegurar a portabilidade da informação	*Risk Map*	- Consiste na incapacidade em assegurar a portabilidade da informação; - Tendo como consequência a incapacidade de transportar a informação dos sistemas para dispositivos móveis; e - Podendo conduzir à perda total/ parcial da informação, em caso de problemas nos sistemas de *backups*.
FR.46	Ambiente Físico	Segurança física inadequada envolvendo *data centers*	*Risk Map*	- Consiste na falta de segurança física de *data centers* adequada; - Tendo como consequência a existência de falhas de segurança que podem levar a intrusões não detetadas; e - Podendo conduzir à perda de informação crítica e dano da infraestrutura física dos *data centers* (*hardware*).

FR.47	Privacidade e Proteção de Dados	Acesso não autorizado a informação pessoal	*Risk Map*	- Consiste na falta de limitação na atribuição de acessos a informação pessoal; - Tendo como consequência o aproveitamento de informação crítica ou confidencial por parte de colaboradores ou elementos externos sem acesso autorizado; e - Conduzindo à perda de informação pessoal e crítica e à fuga da mesma informação para o exterior, pondo em causa a reputação e imagem da empresa.
FR.48	Privacidade e Proteção de Dados	Falta de transparência na classificação e posse da informação	*Risk Map*	- Consiste na incapacidade da classificação e posse da informação de forma transparente; - Tendo como consequência a falta de conhecimento acerca da criticidade e sigilo da informação que pode ser partilhada; e - Podendo conduzir à perda de informação crítica e à fuga da mesma informação para o exterior da empresa.
FR.49	Privacidade e Proteção de Dados	Falta de integridade de informação	*Risk Map*	- Consiste na incapacidade de manter a integridade da informação; - Tendo como consequência a alteração/ eliminação da informação; e - Conduzindo à perda ou alteração de informação.
FR.50	Gestão de Registos	Gestão inapropriada de registos	*Risk Map*	- Consiste na incapacidade de gestão de registos; - Tendo como consequência a inexistência de registos/ *logs* de alterações de registos; e - Podendo conduzir à falta de integridade da informação e à posse não autorizada de informação crítica.
FR.51	Gestão de Registos	Falha em manter segurança	*Risk Map*	- Consiste na incapacidade de manter a segurança dos registos de informação; - Tendo como consequência a incorreta manutenção de integridade e correção dos registos de informação; e - Podendo conduzir a falhas na integridade da informação e posse não autorizada de informação crítica.
FR.52	Gestão de Registos	Inexistência de políticas e procedimentos de retenção de dados	*Risk Map*	- Consiste na falta de políticas e procedimentos de retenção de dados; - Tendo como consequência a inexistência de garantia da realização das atividades definidas de acordo com os objetivos estabelecidos para a retenção de dados; e - Podendo conduzir à não obtenção dos resultados esperados e subsequente falta de informação quando necessária.
FR.53	Descontinuidade e alienação	Recolha de produtos inadequada	*Risk Map*	- Consiste na falta de recolha de produtos adequada; - Tendo como consequência a manutenção de produtos descontinuados/ alienados e sem assistência; e - Podendo conduzir ao descontentamento dos clientes e perda ao nível da receita relativa ao(s) produto(s).
FR.54	Descontinuidade e alienação	Falta de responsabilidade pela pós-venda de produtos, incluindo a sua rutura e eliminação	*Risk Map*	- Consiste na inexistência de responsabilidade pela pós-venda de produtos, incluindo a sua rutura e eliminação; - Tendo como consequência a falta de assistência ao cliente após a venda, rutura e/ ou eliminação de produtos; e - Podendo conduzir ao descontentamento do cliente e falta de confiança na empresa.

FR.55	Inovação, pesquisa e desenvolvimento	Falha para selecionar ideias comercialmente viáveis	*Risk Map*	- Consiste na incorreta seleção de ideias exequíveis comercialmente; - Tendo como consequência a falta de desenvolvimento de novos produtos que vão ao encontro das tendências do mercado em que a empresa se insere; e - Podendo conduzir à perda de receita e de clientes.
FR.56	Inovação, pesquisa e desenvolvimento	Pesquisa inadequada do mercado	*Risk Map*	- Consiste na falta de pesquisa adequada de mercado, nomeadamente no acompanhamento de tendências do mesmo; - Tendo como consequência a falta de inovação e subsequente distinção face à concorrência; e - Podendo conduzir à estagnação de produtos da empresa e à perda de receita.
FR.57	Inovação, pesquisa e desenvolvimento	Protótipos inadequados	*Risk Map*	- Consiste na falta de desenvolvimento de protótipos adequados; - Tendo como consequência o desenvolvimento de novos produtos desadequado face ao desenho dos mesmos; e - Conduzindo à não obtenção dos produtos pretendidos e à insatisfação e perda de clientes, bem como à perda da potencial receita.
FR.58	Desenho/ qualidade do produto	Padrões de qualidade inadequados	*Risk Map*	- Consiste na falta de padrões de qualidade adequados; - Tendo como consequência o desenho de produtos assente em padrões de fraca qualidade; e - Conduzindo a um desenvolvimento deficiente do produto, que não cumpre os requisitos desejados e com a qualidade necessária.
FR.59	Desenho/ qualidade do produto	Desenho de produto e verificação do desenvolvimento ineficazes	*Risk Map*	- Consiste na falta de desenho e verificação do desenvolvimento de produto eficazes; - Tendo como consequência o desenvolvimento de produtos de fraca qualidade e que não vão ao encontro das expectativas do cliente; e - Podendo conduzir ao desenvolvimento de produtos de fraca qualidade, à insatisfação e perda de clientes, bem como ter influência na reputação/ imagem da empresa.
FR.60	Produção	Controlos de qualidade inadequados	*Risk Map*	- Consiste na falta de controlos de qualidade adequados; - Tendo como consequência o desenvolvimento de produtos com fraca qualidade ou mesmo sem qualidade; e - Podendo conduzir à falta de confiança, insatisfação do cliente, má reputação/ imagem da empresa e à perda de receita.
FR.61	Produção	Avaliação técnica inadequada para novos produtos	*Risk Map*	- Consiste na falta de avaliação técnica adequada para novos produtos; - Tendo como consequência a incapacidade de corresponder às expectativas do mercado; e - Podendo conduzir à incapacidade de ir ao encontro das expectativas do cliente e à perda de receita.
FR.62	Produção	Colaboração insuficiente com terceiros	*Risk Map*	- Consiste na falta de colaboração com terceiros; - Tendo como consequência a impossibilidade de aproveitar o conhecimento de terceiros em matérias que poderiam beneficiar a empresa; e - Podendo conduzir ao desenvolvimento de produtos menos célere e inovador e à perda de receita.

FR.63	Teste	Testes de mercado inadequados	*Risk Map*	- Consiste na falta de testes de mercado adequados; - Tendo como consequência o lançamento de produtos sem estudo prévio à aceitação dos mesmos pelo mercado; e - Podendo conduzir à fraca venda dos produtos e à perda de receita com os mesmos, por não irem ao encontro das necessidades dos clientes.
FR.64	Teste	Falha em monitorizar as atividades dos parceiros de negócio	*Risk Map*	- Consiste na incapacidade de monitorizar as atividades dos parceiros de negócio; - Tendo como consequência a receção de produtos, componentes de produtos e/ ou serviços com fraca qualidade; e - Podendo conduzir a falhas de prestação de serviços e/ ou à venda de produtos com deficiências.
FR.65	Relação com clientes/ apoio ao cliente	Infraestrutura inadequada para apoiar os clientes	*Risk Map*	- Consiste na fraca implementação de uma infraestrutura de assistência ao cliente; - Tendo como consequência o aumento do tempo médio de atendimento de clientes e a diminuição da qualidade do serviço prestado; e - Conduzindo à insatisfação de clientes e à sua perda para a concorrência, levando à perda de receita.
FR.66	Relação com clientes/ apoio ao cliente	Fraca definição de *frameworks* de apoio ao cliente, fluxos de trabalho e métricas de desempenho	*Risk Map*	- Consiste na incorreta definição de *frameworks* de assistência a clientes, respectivos fluxos de trabalho e métricas de desempenho; - Tendo como consequência a morosa e incorreta avaliação e tratamento de questões levantadas pelos clientes; e - Podendo conduzir à insatisfação do cliente, à sua perda para a concorrência e respetiva perda de receita.
FR.67	Relação com clientes/ apoio ao cliente	Atenção inadequada à satisfação do cliente	*Risk Map*	- Consiste na falta de atenção adequada à satisfação do cliente; - Tendo como consequência a incapacidade de resposta atempada e adequada às necessidades do cliente, bem como o desperdício de oportunidade para melhorar a qualidade de produtos/ serviços; e - Podendo conduzir à perda de clientes e à respetiva perda de receita.
FR.68	*E-commerce*/ Estratégia de internet	Falta de divulgação de produtos ou serviços na Internet	*Risk Map*	- Consiste na inexistência de divulgação de produtos/ serviços na Internet; - Tendo como consequência a redução da competitividade da empresa no mercado global e inibição do aumento de pontos de distribuição e/ ou venda de produto/ serviços; e - Podendo conduzir à redução de quota de mercado e à perda da potencial receita.
FR.69	Planeamento	Incapacidade em determinar e manter a segurança do armazenamento de *stock*	*Risk Map*	- Consiste na falta de capacidade de determinação e manutenção da segurança do armazenamento de *stock*; - Potenciando a existência de falhas de segurança que podem ser aproveitadas por pessoas mal intencionadas; e - Conduzindo à ocorrência de furtos, danos no *stock* e possível rutura do mesmo, tendo impacto na perda de receita.
FR.70	Planeamento	Proliferação da Unidade de Gestão do Inventário	*Risk Map*	- Consiste no excesso de unidades de gestão do inventário; - Tendo como consequência a dispersão de informação em diferentes plataformas de inventário; e - Podendo conduzir à existência de informação duplicada, tendo impacto na disponibilização de recursos e subsequente perda de receita.

FR.71	Fornecimento	Incapacidade de adquirir bens/ matérias-primas com preços eficientes e em limitar os custos de materiais voláteis	*Risk Map*	- Consiste na falta de capacidade para aquisição de bens/ matérias-primas a preços eficientes e para limitação dos custos de materiais voláteis; - Tendo como consequência o aumento do custo de produção e consequente aumento do preço de venda do produto final; e - Podendo conduzir à redução de vendas de produtos/ serviços (devido a preço elevado exigido aos clientes) e consequente perda de receita.
FR.72	Fornecimento	Processo inadequado de seleção de fornecedores	*Risk Map*	- Consiste na falta de processo adequado de seleção de fornecedores; - Tendo como consequência a seleção de fornecedores menos indicados ou aptos para fornecer os recursos necessários pela empresa; e - Podendo conduzir a ruturas de *stock* e/ ou falha na prestação de serviços, bem como à fraca qualidade de produtos/ serviços, e respetiva perda de receita.
FR.73	Fornecimento	Qualidade inadequada de bens/ matérias-primas	*Risk Map*	- Consiste na falta de qualidade de bens/ matérias-primas; - Potenciando o desenvolvimento de produtos/ serviços que não cumprem a qualidade exigida e a entrega de produtos/ serviços de fraca qualidade; e - Podendo conduzir à quebra de confiança de clientes, ao dano da reputação/ imagem da empresa, com consequente perda de receita.
FR.74	Produção	Processos ineficientes de gestão/ armazenamento de inventário	*Risk Map*	- Consiste na falta de processos eficientes de gestão/ armazenamento de inventário; - Tendo como consequência uma morosa consulta/ identificação de informação relativa aos *stocks* dos recursos; e - Conduzindo à demora ou paragem da produção de produtos/ serviços e subsequente não comercialização de produtos/ serviços.
FR.75	Produção	Falta de flexibilidade de produção para reagir a perturbações	*Risk Map*	- Consiste na falta de meios para ultrapassar perturbações ocorridas na produção; - Tendo como consequência a dificuldade/ impossibilidade de superar as dificuldades encontradas; e - Conduzindo à demora ou paragem da produção de produtos/ serviços e subsequente não comercialização de produtos/ serviços.
FR.76	Entrega	Prestadores de serviço logísticos não fiáveis	*Risk Map*	- Consiste na realização de contractos com prestadores de serviços não fiáveis; - Tendo como consequência o atraso/ falha na entrega de produtos/ serviços a clientes e respetiva insatisfação dos mesmos; e - Podendo conduzir à perda de clientes e subsequente perda de receita.
FR.77	Entrega	Falha em otimizar o prazo de entrega para armazenamento/ distribuição	*Risk Map*	- Consiste na falta de capacidade para otimizar o prazo de entrega para armazenamento e distribuição; - Tendo como consequência a falta de *stock* nos pontos de venda e atrasos/ falhas na entrega de produtos/ serviços a clientes e respectiva insatisfação dos mesmos; e - Podendo conduzir à perda de clientes e subsequente perda de receita.

FR.78	Entrega	Desenho de rede inapropriado	*Risk Map*	- Consiste numa conceção inapropriada do desenho de rede; - Tendo como consequências a não deteção de pontos de falha no processo de entrega de produtos/ serviços e atrasos nos prazos de entrega de produtos/ serviços; e - Conduzindo à insatisfação de clientes, podendo levar à perda dos mesmos e à respectiva perda de receita.
FR.79	Entrega	Processo ineficiente de verificação e gestão de pedidos	*Risk Map*	- Consiste na falta de processo eficiente de verificação e gestão de pedidos; - Tendo como consequência falhas na resposta às necessidades de clientes e insatisfação dos mesmos; e - Podendo conduzir à perda de clientes e subsequente perda de receita.
FR.80	Entrega	Processo ineficiente de inventário e canais de distribuição	*Risk Map*	- Consiste na falta de processo eficiente de inventário e de canais de distribuição; - Tendo como consequência a utilização desnecessária de recursos e a não disponibilização de produtos nas quantidades necessárias; e - Conduzindo à insatisfação dos clientes, aumento do custo de distribuição e perda de receita.
FR.81	Conformidade com normas e políticas de contabilidade	Incapacidade de monitorizar e implementar padrões	*Risk Map*	- Consiste na falta de capacidade para monitorização e implementação padrões de *reporting*; - Tendo como consequência a inconsistência na elaboração e emissão de relatórios; e - Podendo conduzir ao incumprimento das normas e políticas de contabilidade e perda do foco principal dos relatórios.
FR.82	Conformidade com normas e políticas de contabilidade	Incapacidade de implementar as normas internacionais de *reporting* financeiro	*Risk Map*	- Consiste na falta de capacidade para implementação de normas internacionais de *reporting* financeiro; - Tendo como consequência a elaboração de relatórios não uniformizados e legíveis por todos os parceiros de negócio; e - Podendo conduzir à elaboração de relatórios suscetíveis à colocação sobre questões de veracidade.
FR.83	Conformidade com normas e políticas de contabilidade	Políticas inapropriadas de contabilidade	*Risk Map*	- Consiste na falta de políticas apropriadas de contabilidade; - Tendo como consequência a elaboração de relatórios contabilísticos desviados do objetivo, devido ao não cumprimento de normas de contabilidade; e - Podendo conduzir relatórios pouco objetivos e sem o conteúdo e formato exigidos.
FR.84	Conformidade com normas e políticas de contabilidade	Falta de conhecimentos das políticas de contabilidade	*Risk Map*	- Consiste no desconhecimento das políticas de contabilidade; - Tendo como consequência a elaboração de relatórios não-alinhados com as políticas de contabilidade; e - Podendo conduzir relatórios pouco objetivos e sem o conteúdo e formato exigidos.
FR.85	Fraude de demonstrações financeiras	Inadequada gestão corporativa	*Risk Map*	- Consiste na falta de gestão corporativa adequada; - Tendo como consequência a impossibilidade de garantir que são cumpridos todos os padrões organizacionais e legais da empresa; e - Conduzindo a um clima de desconfiança à forma como a empresa é gerida, devido à possibilidade de existência de fraude de demonstrações financeiras.
FR.86	Fraude de demonstrações financeiras	Programas inefetivos antifraude	*Risk Map*	- Consiste na falta de programas efetivos antifraude; - Tendo como consequência a impossibilidade de conhecimento e deteção de ações fraudulentas; e - Podendo conduzir à realização de ações fraudulentas, sem que seja encontrado o responsável pelas mesmas.

FR.87	Fraude de demonstrações financeiras	Incapacidade de implementar um programa de ética e conformidade	*Risk Map*	- Consiste na falta de capacidade para implementar um programa de conformidade e ética; - Tendo como consequência a elaboração de relatórios adulterados/ pouco éticos e em não conformidade com as políticas e regulamentos da empresa; e - Podendo conduzir à descredibilização da empresa.
FR.88	Fraude de demonstrações financeiras	Falta de controlos internos efetivos	*Risk Map*	- Consiste na inexistência de controlos internos efetivos; - Tendo como consequência a não deteção de incorreções financeiras e a consequente falta de informação crítica coerente e fiável nos relatórios elaborados; e - Podendo conduzir a situações de fraude/ corrupção devido à falta de reporte de incorreções.
FR.89	Fraude de demonstrações financeiras	Falha na implementação da segregação de funções	*Risk Map*	- Consiste na incorreta implementação de segregação de funções; - Tendo como consequência a não definição e separação das funções de cada colaborador na realização das atividades de *reporting*, que devem ser realizadas por colabores distintos; e - Podendo conduzir a casos de fraude/ corrupção no que respeita à elaboração/ emissão de relatórios.
FR.90	Qualidade de *Reporting*	Falha no fornecimento de informações precisas e completas	*Risk Map*	- Consiste na falta de precisão e completude da informação fornecida; - Tendo como consequência a elaboração de relatórios com informação pouco consistente e suscetível de diversas interpretações; e - Podendo conduzir à elaboração/ emissão de relatórios que não reflitam a realidade da empresa, pondo em causa a reputação da mesma perante os *stackholders*.
FR.91	Qualidade de *Reporting*	Falha no fornecimento de informações em tempo útil	*Risk Map*	- Consiste na indisponibilidade de informação em tempo útil; - Tendo como consequência a elaboração de relatórios sem informação relevante ou não atualizada; e - Podendo conduzir à falta de qualidade, conteúdo e precisão dos relatórios.
FR.92	Qualidade de *Reporting*	Utilização de informação e ferramentas de *reporting* desatualizadas	*Risk Map*	- Consiste na utilização de informação e ferramentas desatualizadas na elaboração de *reporting*; - Tendo como consequência a elaboração de relatórios que não estão atualizados com a realidade da empresa; e - Podendo conduzir à falta de qualidade, conteúdo e precisão dos relatórios.

Anexo 3 – Riscos, OC e AC dos SI/ TI

A tabela que se encontra apresentada em baixo, contem os riscos dos SI/ TI, devidamente detalhados com base nos riscos anteriormente identificados. Adicionalmente, na tabela também está apresentado os respetivos objetivos e atividades de controlo.

Risco		Objetivos de controlo		Atividades de Controlo	
ID	**Descrição risco**	**ID**	**Descrição OC**	**ID**	**Descrição AC**
Gestão de Operações					
RS.01 [FR.42,	Sistemas de produção, programas, e/ou postos de	OPER.01	A gestão de operações é apropriada para suportar a calendarização, execução,	OP.01	Está formalmente definido um procedimento de gestão de operações.

FR.43, FR.50, FR.51]	trabalho resultam em processamento de dados imprecisos, incompletos e não autorizados.		monitorização, e continuidade dos programas e processos de TI para um completo, eficiente e valido processamento e registo das transações de informação.	OP.02	O acesso à calendarização de *jobs*/*batch* é restrito aos colaboradores autorizados.
				OP.03	Alteração de *jobs*/*batch* é devidamente documentada e aprovada.
				OP.04	Estão definidos procedimentos formais para garantir que o processamento de *jobs*/*batch* (incluindo interfaces) é monitorizado e as exceções são devidamente acompanhadas e resolvidas (mecanismo de controle de exceções).
RS.02 [FR.52; FR.44; FR.45; FR.50; FR.51]	Os dados financeiros não podem ser recuperados ou acedidos em tempo útil quando há uma perda de dados.	OPER.02	Os dados são geridos de forma a assegurar que a informação se mantém completa, correta e valida durante o processo de *backup*, de forma a estar assegurado a recuperação da informação em caso de necessidade.	OP.05	Estão definidos procedimentos para a realização de *backups*, incluindo procedimentos de monitorização dos backups para deteção e resolução de erros.
				OP.06	Os *backups* devem ser geridos (e.g. períodos de retenção) tendo em consideração a criticidade da informação para o negócio.
				OP.07	O acesso à calendarização de jobs de *backup* é restrito aos colaboradores autorizados.
				OP.08	Estão definidos procedimentos formais para garantir que o processamento de jobs de *backup* é monitorizado e as exceções são devidamente acompanhadas e resolvidas (mecanismo de controle de exceções).
				OP.09	Os *backups* são arquivados em localizações alternativas (*off-site*) para minimizar o risco de perda de dados.
				OP.10	Devem ser efetuados periodicamente testes de *restores* às tapes de *backups*.
Segurança da Informação					
RS.03 [FR.40; FR.48; FR.46; FR.47; FR.41]	A gestão de acesso não respeita os requisitos de negócio comprometendo a segurança de sistemas críticos para os negócios.	SEG.01	A segurança dos sistemas é corretamente implementada, administrada e registada de forma a evitar o acesso/ modificações de programas ou dados que resultem num incompleto, incorreto ou invalido processamento/ registo da informação.	SG.01	Está formalmente definida uma política de segurança de informação.
				SG.02	Está formalmente definida uma política de atribuição de nomes de utilizadores únicos para gestão dos acessos.
				SG.03	Estão formalmente definidos procedimentos de gestão de acessos (i.e. criação, alteração, suspensão e revisão), para os acessos à rede, aos sistemas, e às bases de dados.
				SG.04	A saída/ alteração de funções de colaboradores é devidamente comunicada para que possam ser eliminados/ ajustados os acessos.
				SG.05	Os acessos às aplicações, sistemas operativos e bases de dados são revistos periodicamente pelos *owners* dos dados.

				SG.11	Os acessos devem ser atribuídos/ revistos tendo em consideração os conflitos de segregação de funções definidos. As exceções são prontamente corrigidas.
				SG.18	A atribuição de acessos de um colaborador às aplicações/ rede da operadora é devidamente aprovada.
RS.04 [FR.47; FR.37; FR.38]	Os sistemas não são adequadamente configurados ou atualizados para restringir o acesso do sistema para utilizadores devidamente autorizados e adequados.	SEG.02	As configurações de segurança de programas e sistemas são geridas de forma eficiente para prevenir alterações, a programas e dados, não autorizadas que possam por em risco o completo e correto processamento de informação.	SG.07	Os privilégios de acesso "super user" / administrador nas aplicações e bases de dados apenas é atribuído quando realmente necessário e todas as ações são registadas e revistas pela gestão.
				SG.08	Estão implementados controlos de forma a identificar univocamente o utilizador responsável pelas operações realizadas nas aplicações e bases de dados (user ids únicos e não partilhados, logs).
				SG.09	Estão definidos parâmetros de autenticação (e.g., Password *Minimum Length* & *Complexity*, *Password Expiration, Account* Lockout, etc.) para acesso às aplicações e bases de dados.
				SG.10	Existe *software* antivírus instalado nos computadores ligados à rede para garantir a segurança dos sistemas, programas e dados evitando alterações não autorizadas. A lista de vírus conhecidos é atualizada adequadamente e regularmente. Todos os programas e ficheiros existentes na rede são verificados regularmente.
				SG.17	Existe uma segregação e controlo da rede da Empresa, protegendo os diferentes ambientes e sistemas de acessos não autorizados.
RS.05 [FR.40; FR.18]	Pessoas obtêm acesso inadequado ao equipamento no centro de dados e exploram esse acesso para contornar os controlos de acesso lógico e ter acesso inadequado aos sistemas.	SEG.03	Os acessos físicos são geridos de forma a proteger a integridade da informação e garantir que esta é mantida e guardada com recurso aos componentes corretos da infraestrutura de tecnologias de informação.	SG.12	Existem procedimentos formais de controlo dos acessos físicos, que permitem restringir e registar os acessos a localizações com informação crítica.
				SG.13	Existem procedimentos formais de gestão dos acessos físicos (i.e. criação, alteração, suspensão e revisão de acessos) e estão definidas e atribuídas responsabilidades, de forma a que apenas um número limitado de pessoas pode efetuar alterações às autorizações.
				SG.14	A saída/alteração de funções de colaboradores é comunicada para que possam ser eliminados/ajustados os acessos físicos à informação.
RS.06 [FR.04;	Os dados financeiros não podem ser recuperados ou	SEG.04	O sistema é resiliente a falhas catastróficas, acidentais ou intencionais.	SG.15	Está definido um plano de continuidade de negócio e um plano de recuperação de desastres.

FR.05; FR.25]	acedidos em tempo útil quando há uma perda de dados.			SG.16	Está definido um plano de que contemple a segurança física do CPD, existem fontes de alimentação alternativas (e.g. fornecimento de energia ininterrupto, geradores, etc) e controlos de proteção do ambiente de processamento.
Gestão de Alterações					
RS.07 [FR.30; FR.31; FR.32; FR.33; FR.39]	São efetuadas alterações inadequadas para sistemas de aplicações ou programas que contêm controlos relevantes automatizados (i.e., definições configuráveis, algoritmos automatizados, cálculos automatizados e extração de dados automatizada) e / ou relatórios lógicos.	ALTER. 01	Os programas e sistemas são adequadamente modificados para suportar o processamento e registo da informação de forma correta, completa e válida.	ALT.01	É utilizada uma metodologia ou processo, devidamente aprovado, relativo à modificação dos sistemas aplicacionais de forma a garantir consistência no desenvolvimento da alteração.
				ALT.02	As alterações às aplicações e bases de dados são aprovadas.
				ALT.03	Alterações às aplicações e bases de dados são devidamente testadas de forma a garantir que estão em conformidade com os requisitos definidos.
				ALT.04	Os ambientes de desenvolvimento, QA e Produtivo estão devidamente segregados.
Fornecedores externos					
RS.09 [FR.06]	Risco contratual	FOR.01	Garantir que o contrato entre a operadora e o parceiro de negócio se encontra em vigor	FR.01	O contrato entre a operadora e o parceiro de negócio e revisto anualmente, por ambas as partes.

Riscos – Integração

Risco		Objectivos de controlo		Actividades de Controlo	
ID Risco	**Descrição risco**	**ID OC**	**Descrição OC**	**ID**	**Descrição AC**
Integração da Informação - Consumos & Carregamentos					

		Consumos			
RS.10	Falta de integridade da informação financeira	OC.01	Garantir que a informação de consumos de saldo em números pré-pagos GSM é corretamente integrada contabilidade	AC.01	Estão implementados controlos à informação extraída do sistema Billing GSM
				AC.02	Estão implementados controlos antes da integração da informação na contabilidade.
				AC.03	Estão implementados controlos à integridade da informação que foi integrada na contabilidade.
		Carregamentos			
		OC.02	Garantir que a informação dos carregamentos de saldo em números pré-pagos GSM é corretamente integrada contabilidade	AC.04	Estão implementados controlos à informação extraída do sistema Billing GSM
				AC.05	Estão implementados controlos antes da integração da informação na contabilidade.
				AC.06	Estão implementados controlos à integridade da informação que foi integrada na contabilidade.

Anexo 4 – Pedidos de informação

# ID Pedido	Informação a Solicitar	Amostra	Responsável	Estado
Geral				
GER.01	Organograma da área de SI	N/A	DSI	Recebido
GER.02	Diagrama de Rede	N/A	DSI	Não existe
GER.03	Contrato entre o parceiro de negócio e a operadora	N/A	DSI	Recebido
GER.04	Procedimentos de gestão de *helpdesk*	N/A	DSI	Não existe
GER.05	Listagem dos atuais colaboradores da operadora (proveniente dos RH) com a seguinte informação: - Número de Colaborador; - Nome; - Data de entrada; e - Direção/Área.	N/A	DSI	Não existe

GER.06	Listagem de colaboradores que saíram dos quadros da Empresa durante 2014, com a seguinte informação: - Número de colaborador; - Nome; - Data de saída da empresa; e - Direção/Área.	N/A	DSI	Não existe
Gestão de operações *e CPD*				
OPER.01	Procedimentos de gestão de *jobs* / *batchs* aplicacionais (e.g. responsáveis pela aprovação dos jobs, calendarização, monitorização e tratamento)	N/A	DSI	Não existe
OPER.02	Procedimento de gestão de *backups*	N/A	DSI	Recebido
OPER.03	Procedimento de envio das tapes e disco de *backup* para *off-site*	N/A	DSI	Não existe
OPER.04	Evidência do envio dos *backups* para *off-site*.	N/A	DSI	Não existe
OPER.05	Listagem das bases de dados das aplicações da operadora [Servidor | Base de dados | Aplicação], nomeadamente: Billing GSM, Cobranças e Contabilidade.	N/A	DSI	Recebido
OPER.06	Matriz de classificação da informação	N/A	DSI	Não existe
OPER.07	Evidências de testes de *restore* às tapes de *backups* realizados em 2014.	N/A	DSI	Não existe
OPER.08	Listagem dos utilizadores (incluindo perfis) com permissão para criação, alteração ou eliminação de jobs de *backups* (e.g. servidor alvo, aplicação, informação, tipo de backup, calendarização, período de retenção).	N/A	DSI	Recebido
OPER.09	Listagem de alterações aos jobs de *backup*, durante 2014.	N/A	DSI	Não existe
OPER.10	Aprovação da alteração aos *jobs* de *backups*, para uma amostra de alterações a selecionar de OPER.08.	N/A	DSI	N/A
Billing GSM				
OPER.11	Listagem dos utilizadores com permissão para criação, alteração ou remoção de jobs operacionais (e.g. calendarização, operações), extraída dos sistema Billing GSM.	N/A	DSI	Recebido
OPER.12	Configurações dos *jobs*/ *batches* definidos nos sistema de Billing GSM (ambiente produtivo), incluindo a sua calendarização.	N/A	DSI	Recebido
OPER.13	Relatórios da monitorização efetuada ao processamento dos jobs operacionais nos sistemas de Billing GSM, durante 2014.	N/A	DSI	Não existe
OPER.14	Logs e alertas emitidos no processamento de jobs operacionais do sistema de Billing GSM, para os dias definido para a amostra (ver coluna: "Amostra").	Dias: 2-Fev 8-Fev 15-Fev 8-Mar 11-Mar 22-Abr 23-Jul 24-Jul 7-Ago 13-Ago 28-Ago 3-Out 20-Out 8-Nov 17-Nov	DSI	Não existe
OPER.15	Billing GSM - Com base nos *logs* de execução dos jobs/ *batches* selecionados, caso existam erros iremos solicitar evidências do: - pedido de resolução; e - respectiva resolução.	N/A	DSI	Não existe

OPER.16	Configuração dos *backups* no sistema de Billing GSM (e.g. *print screen)*, incluindo a seguinte informação calendarização, tipo de *backup*, etc.	N/A	DSI	Recebido
OPER.17	Log dos *backups* diários do sistema Billing GSM, para os dias definidos para a amostra (ver coluna: "Amostra")	Dias: 2-Fev 8-Fev 15-Fev 8-Mar 11-Mar 22-Abr 23-Jul 24-Jul 7-Ago 13-Ago 28-Ago 3-Out 20-Out 8-Nov 17-Nov	DSI	Não existe
OPER.18	Evidência da monitorização (e.g. relatório; alertas recebidos) realizada ao processamento dos *backups* do sistema Billing GSM.	N/A	DSI	Não existe
OPER.20	Listagem de alterações aos jobs operacionais, durante 2014, no sistema Billing GSM.	N/A	DSI	Não existe
OPER.21	Aprovação da alteração aos jobs operacionais, para uma amostra de alterações a selecionar de OPER.17	N/A	DSI	Não existe
Cobranças				
OPER.22	Listagem dos utilizadores com permissão para criação, alteração ou remoção de jobs operacionais (e.g. calendarização, operações), extraída do sistema de Cobranças.	N/A	DSI	Recebido
OPER.23	Configurações dos *jobs/ batches* definidos nos sistema de Cobranças (ambiente produtivo), incluindo a sua calendarização.	N/A	DSI	Recebido
OPER.24	Relatórios da monitorização efetuada ao processamento dos jobs operacionais no sistema de Cobranças, durante 2014.	N/A	DSI	Não existe
OPER.25	Logs e alertas emitidos no processamento de *jobs* operacionais do sistema de Cobranças, para os dias definido para a amostra (ver coluna: "Amostra").	Dias: 2-Fev 4-Fev 8-Fev 15-Fev 17- Fev 20- Fev 22-Fev 01-Mar 06-Mar 09-Mar 11-Mar 19-Mar 21-Mar 25-Mar 27-Mar	DSI	Recebido
OPER.26	Cobranças - Com base nos *logs* de execução dos jobs/ *batches* selecionados, caso existam erros iremos solicitar evidências do: - pedido de resolução; e - respectiva resolução.	Dias: 8 Fev e 25-Mar	DSI	Não existe
OPER.27	Configuração dos *backups* no sistema de Cobranças (e.g. *print screen)*, incluindo a seguinte informação calendarização, tipo de *backup*, etc.	N/A	DSI	Recebido
OPER.28	Evidência da monitorização (e.g. relatório; alertas recebidos) realizada ao processamento dos *backups* do sistema Cobranças.	N/A	DSI	Não existe
OPER.29	Log dos *backups* diários do sistema Cobranças, para os dias definidos para a amostra (ver coluna: "Amostra")	Dias: 2-Fev 8-Fev 15-Fev 8-Mar 11-Mar 22-Abr 23-Jul 24-Jul 7-Ago 13-Ago 28-Ago 3-Out 20-Out 8-Nov 17-Nov	DSI	Não existe
OPER.30	Listagem de alterações aos jobs operacionais, durante 2014, no sistema Cobranças.	N/A	DSI	Não existe

OPER.31	Aprovação da alteração aos jobs operacionais, para uma amostra de alterações a selecionar de OPER.27	N/A	DSI	Não existe
Contabilidade				
OPER.32	Listagem dos utilizadores com permissão para criação, alteração ou remoção de jobs operacionais (e.g. calendarização, operações), extraída do sistema de Contabilidade.	N/A	DSI	Recebido
OPER.33	Configurações dos *jobs/ batches* definidos nos sistema de Contabilidade (ambiente produtivo), incluindo a sua calendarização.	N/A	DSI	Recebido
OPER.34	Relatórios da monitorização efetuada ao processamento dos jobs operacionais nos sistemas de Contabilidade, durante 2014.	N/A	DSI	Não existe
OPER.35	Logs e alertas emitidos no processamento de jobs operacionais do sistema de Contabilidade, para os dias definido para a amostra (ver coluna: "Amostra").	Dias: 2-Fev 4-Fev 8-Fev 15-Fev 17- Fev 20- Fev 22-Fev 01-Mar 06-Mar 09-Mar 11-Mar 19-Mar 21-Mar 25-Mar 27-Mar	DSI	Recebido
OPER.36	Contabilidade - Com base nos *logs* de execução dos jobs/ *batches* selecionados, caso existam erros iremos solicitar evidências do: - pedido de resolução; e - respectiva resolução.	Log do dia 2-Fev 15-Fev 09-Mar e 27-Mar	DSI	Recebido
OPER.37	Configuração dos *backups* no sistema de Contabilidade (e.g. *print screen)*, incluindo a seguinte informação calendarização, tipo de *backup*, etc.	N/A	DSI	Recebido
OPER.38	Log dos *backups* diários do sistema Contabilidade, para os dias definidos para a amostra (ver coluna: "Amostra")	Dias: 2-Fev 8-Fev 15-Fev 8-Mar 11-Mar 22-Abr 23-Jul 24-Jul 7-Ago 13-Ago 28-Ago 3-Out 20-Out 8-Nov 17-Nov	DSI	Não existe
OPER.39	Evidência da monitorização (e.g. relatório; alertas recebidos) realizada ao processamento dos *backups* do sistema Contabilidade.	N/A	DSI	Não existe
OPER.40	Listagem de alterações aos jobs operacionais, durante 2014, no sistema Contabilidade.	N/A	DSI	Não existe
OPER.41	Aprovação da alteração aos jobs operacionais, para uma amostra de alterações a selecionar de OPER.37	N/A	DSI	Não existe
Segurança da Informação				
SEG.01	Política de segurança da informação	N/A	DSI	Recebido
SEG.02	Procedimento de gestão e revisão de acessos (criação, alteração e eliminação) dos sistemas em âmbito (Billing GSM, Cobranças e Contabilidade).	N/A	DSI	Não existe
SEG.03	Procedimento/ política de gestão de acessos físicos às instalações e CPD.	N/A	DSI	Não existe
SEG.04	Procedimentos de gestão de acessos remotos, VPN, (i.e. criação, alteração, suspensão e revisão).	N/A	DSI	Não existe
SEG.05	Procedimentos de gestão de acessos (i.e. criação, alteração, suspensão e revisão) à rede da operadora (*active directory).*	N/A	DSI	Não existe

SEG.06	Lista de colaboradores autorizados a aceder ao Centro de Processamento de Dados (CPD).	N/A	DSI	Recebido
SEG.07	Log de acesso ao CPD para os meses definidos na amostra (ver coluna "Amostra")	Meses: Janeiro e Março	DSI	Recebido
SEG.08	Regras de nomenclatura na criação dos utilizadores com acesso aos sistemas em âmbito (Billing GSM, Cobranças e Contabilidade) e rede.	N/A	DSI	Não existe
SEG.09	Matriz com regras de segregação de funções relativas ao sistemas de informação (Billing GSM, Cobranças e Contabilidade).	N/A	DSI	Não existe
SEG.10	Evidência da comunicação, por parte do RH, da saída ou alteração de funções de uma amostra de colaboradores/ consultores externos que deixaram de exercer as respetivas funções, a selecionar posteriormente de GER.06	N/A	DSI	N/A
SEG.11	Relatórios das revisões periódicas dos logs/ registos de acessos físicos ao CPD.	N/A	DSI	Não existe
SEG.12	Aprovação dos acessos físicos ao CPD, dos colaboradores selecionados na amostra (ver coluna: 'Amostra')	Ver sheet amostra:'Users CPD'	DSI	Não existe
SEG.13	Evidência da comunicação, por parte do RH, da saída ou alteração de funções de uma amostra de colaboradores/ consultores externos que deixaram de exercer as respetivas funções, a selecionar posteriormente de GER.07	N/A	DSI	N/A
SEG.14	Plano de Continuidade de Negócio (inclusive Plano Recuperação de Desastre)	N/A	DSI	Não existe
SEG.15	Parâmetros de segurança (e.g. segurança das *passwords*, bloqueios de contas), da *Active Directory* e sistema Contabilidade.	N/A	DSI	Recebido
SEG.16	Procedimentos de antivírus: - Calendarização; - Monitorização do estado/ resolução de situações; e - Atualização periódica.	N/A	DSI	Recebido
SEG.17	Evidências (e.g. *print-screens*; relatórios dos antivírus) de que o antivírus se encontra: - Ativo; - Atualizado; - Configuração dos *scans* periódicos; - Resultado dos scans nos diversos computadores.	N/A	DSI	Recebido
Active Directory				
SEG.18	Listagem de utilizadores ativos na *Active Directory* incluindo data de criação e respectivos grupos de acesso (nomeadamente *domain admin*)	N/A	DSI	Recebido
SEG.19	Evidência (e.g. *print screen*) dos parâmetros de segurança da *Active Directory:* *- Password Policies; e* *- Account Lockout.*	N/A	DSI	Recebido
SEG.20	Relatórios de revisão de acessos trimestrais, realizadas durante 2014, à rede (e.g. *active directory).*	N/A	DSI	Não existe
SEG.21	Evidências do processo de pedido/ atribuição de acessos ao *Active Directory*, nomeadamente: (i) pedido de acesso; (ii) aprovação do acesso; para os colaboradores selecionados como amostra. (Amostra a ser definida depois da receção da listagem de utilizadores do *Active Directory*)	Ver sheet amostra: 'Users AD'		Recebido

Billing GSM				
SEG.22	'Listagem de utilizadores e respectivos perfis de acesso às BD's e sistema operativo do sistema Billing GSM.	N/A	DSI	Recebido
SEG.23	Listagem de utilizadores do sistema Billing GSM incluindo data de criação e respectivos perfis de acesso.	N/A	DSI	Recebido
SEG.24	Evidências da revisão de acessos aplicacionais e BD realizada aos *users* do sistema Billing GSM em 2014.	N/A	DSI	Não existe
SEG.25	Evidência (e.g. *print screen*) dos parâmetros de segurança do sistema Billing GSM (e.g. configurações de passwords, bloqueios de contas).	N/A	DSI	Não existe
SEG.26	Evidências do processo de pedido/ atribuição de acessos ao sistema Billing GSM, nomeadamente: (i) pedido de acesso; (ii) aprovação do acesso; para os colaboradores selecionados como amostra. (Amostra a ser definida depois da receção da listagem de utilizadores do sistema de Billing GSM)	Ver sheet: "Amostra Acessos Billing GSM"	DSI	Não existe
Cobranças				
SEG.27	Listagem de utilizadores e respectivos perfis de acesso às BD's e sistema operativo do sistema Cobranças.	N/A	DSI	Recebido
SEG.28	Listagem de utilizadores do sistema de Cobranças incluindo data de criação e respectivos perfis de acesso.	N/A	DSI	Recebido
SEG.29	Evidências da revisão de acessos aplicacionais e BD realizada aos *users* do sistema de Cobranças em 2014.	N/A	DSI	Não existe
SEG.30	Evidência (e.g. *print screen*) dos parâmetros de segurança do sistema Cobranças (e.g. configurações de passwords, bloqueios de contas).	N/A	DSI	Não existe
SEG.31	Evidências do processo de pedido/ atribuição de acessos ao sistema de Cobranças, nomeadamente: (i) pedido de acesso; (ii) aprovação do acesso; para os colaboradores selecionados como amostra. (Amostra a ser definida depois da receção da listagem de utilizadores do sistema de Cobranças)	Ver sheet: "Amostra Acessos Cobranças"	DSI	Recebido
Contabilidade				
SEG.32	Listagem de utilizadores e respectivos perfis de acesso às BD's e sistema operativo do sistema Contabilidade.	N/A	DSI	Não existe
SEG.33	Listagem de utilizadores do sistema de Contabilidade incluindo data de criação e respectivos perfis de acesso.	N/A	DSI	Recebido
SEG.34	Evidências da revisão de acessos aplicacionais e BD realizada aos *users* do sistema de Contabilidade em 2014.	N/A	DSI	Não existe
SEG.35	Evidência (e.g. *print screen*) dos parâmetros de segurança do sistema Contabilidade (e.g. configurações de passwords, bloqueios de contas).	N/A	DSI	Não existe
SEG.36	Evidências do processo de pedido/ atribuição de acessos ao sistema de Contabilidade, nomeadamente: (i) pedido de acesso; (ii) aprovação do acesso; para os colaboradores selecionados como amostra. (Amostra a ser definida depois da receção da listagem de utilizadores do sistema de Cobranças)	Ver sheet: "Amostra Acessos Cobranças"	DSI	Recebido

Gestão de alterações				
ALT.01	Procedimento de gestão de alterações aos sistemas de informação.	N/A	DSI	Recebido
Billing GSM				
ALT.02	Listagem de alterações (manutenção evolutiva e corretiva) relativas ao sistema Billing GSM, concluídas durante o ano de 2014.	N/A	DSI	Recebido
ALT.03	Listagem de alterações à base de dados de suporte ao sistema Billing GSM *(updates*, instalações de *patches*) ocorridas durante o ano de 2014 (com informação da data de início e data de fim)	N/A	DSI	Não existe
ALT.04	Listagem de alterações ao sistema operativo do sistema Billing GSM *(updates*, instalações de *patches*) ocorridas durante o ano de 2014 (com informação da data de início e data de fim)	N/A	DSI	Recebido
ALT.05	Para as alterações do sistema e base de dados do Billing GSM selecionadas como amostra (ver coluna amostra), obter a seguinte documentação: - Pedido de alteração; - Aprovação formal da alteração; - Documentação da especificação funcional/ requisitos; - Plano de testes; - Relatórios com resultados dos testes; - Aprovação dos testes de aceitação; e - Pedido e aprovação da passagem a produção.	Ver sheet: 'Alt. Billing GSM'	DSI	Recebido
ALT.06	Para uma amostra selecionada a partir da listagem de alterações do SO do sistema Billing GSM necessitamos: - Evidência da instalação em qualidade antes de produção - Evidência dos testes/ monitorização realizados ao SI de forma a garantir que não teve impacto negativo - Aprovação para entrada em produção.	Ver sheet: 'Alt. SO Billing GSM'	DSI	Não existe
Cobranças				
ALT.07	Listagem de alterações (manutenção evolutiva e corretiva) relativas ao sistema Cobranças, concluídas durante o ano de 2014.	N/A	DSI	Recebido
ALT.08	Listagem de alterações à base de dados de suporte ao sistema Cobranças *(updates*, instalações de *patches*) ocorridas durante o ano de 2014 (com informação da data de início e data de fim)	N/A	DSI	Não existe
ALT.09	Listagem de alterações ao sistema operativo do sistema Cobranças *(updates*, instalações de *patches*) ocorridas durante o ano de 2014 (com informação da data de início e data de fim)	N/A	DSI	Recebido

ALT.10	Para as alterações do sistema e base de dados do Cobranças selecionadas como amostra (ver coluna amostra) , obter a seguinte documentação: - Pedido de alteração; - Aprovação formal da alteração; - Documentação da especificação funcional/ requisitos; - Plano de testes; - Relatórios com resultados dos testes; - Aprovação dos testes de aceitação; e - Pedido e aprovação da passagem a produção.	Ver sheet: 'Alt. Cobranças'	DSI	Recebido
ALT.11	Para uma amostra selecionada a partir da listagem de alterações do SO do sistema Cobranças necessitamos: - Evidência da instalação em qualidade antes de produção - Evidência dos testes/ monitorização realizados ao SI/ TI de forma a garantir que não teve impacto negativo - Aprovação para entrada em produção.	Ver sheet: 'Alt. SO Cobranças'	DSI	Não existe
Contabilidade				
ALT.12	Listagem de alterações (manutenção evolutiva e corretiva) relativas ao sistema Contabilidade, concluídas durante o ano de 2014.	N/A	DSI	Recebido
ALT.13	Listagem de alterações à base de dados de suporte ao sistema Contabilidade (updates, instalações de *patches*) ocorridas durante o ano de 2014 (com informação da data de início e data de fim)	N/A	DSI	Não existe
ALT.14	Listagem de alterações ao sistema operativo do sistema Contabilidade *(updates*, instalações de *patches*) ocorridas durante o ano de 2014 (com informação da data de início e data de fim)	N/A	DSI	Recebido
ALT.15	Para as alterações do sistema Contabilidade selecionadas como amostra (ver coluna amostra), obter a seguinte documentação: - Pedido de alteração; - Aprovação formal da alteração; - Documentação da especificação funcional/ requisitos; - Plano de testes; - Relatórios com resultados dos testes; - Aprovação dos testes de aceitação; e - Pedido e aprovação da passagem a produção.	Ver sheet: 'Alt. Contabilidade'	DSI	Recebido
ALT.16	Para uma amostra selecionada a partir da listagem de alterações do SO do sistema Contabilidade necessitamos: - Evidência da instalação em qualidade antes de produção - Evidência dos testes/ monitorização realizados ao SI/TI de forma a garantir que não tiveram impacto negativo - Aprovação para entrada em produção.	Ver sheet: 'Alt. SO Contabilidade'	DSI	Não existe

ALT.17	Evidência dos testes/ relatórios de testes (técnicos e de aceitação) realizados às bases de dados dos sistemas em âmbito (Billing GSM, Contabilidade e Cobranças), para a amostra de alterações selecionadas (ver sheet:'Amostra')	N/A	DSI	Recebido

Pedido de informação – Integração

# ID Pedido	Informação a Solicitar	Responsável	Estado
Carregamentos & Consumos			
INT.01	Log da interface de integração das cobranças e dos consumos (log NPP)	DSI	Recebido
INT.02	Tabela "General Ledger"	DSI	Recebido
INT.03	Ficheiro com o resumo dos carregamentos (*Billing_recharge_resume*)	DSI	Recebido
INT.04	Ficheiro com o detalhe dos carregamentos (*Billing_recharge_detail*)	DSI	Recebido
INT.05	Ficheiro com o resumo dos consumos (*Billing_usage_resume*)	DSI	Recebido
INT.06	Ficheiro com o detalhe dos consumos (*Billing_usage_detail*)	DSI	Recebido
INT.07	Listagem dos produtos de carregamento definidos no sistema Billing GSM, com a respectiva descrição.	DSI	Recebido
INT.08	Listagem produtos de consumo do sistema Billing GSM e sua caracterização.	DSI	Recebido
INT.09	Tabela de mapeamento entre os produtos definidos no sistema Billing GSM com os produtos/ recursos definidos na Contabilidade	DSI	Recebido
INT.10	Listagem produtos na Contabilidade e sua caracterização	DSI	Recebido
INT.11	Listagem de produtos/ eventos que são excluídos no processo de integração	DSI	Recebido

Anexo 5 – Matriz de testes

Os testes apresentados, encontram-se documentados na primeira pessoa do plural. Os testes foram realizados por apenas uma pessoa, no entanto foram revistos e explicados pelos elementos hierárquicos superiores. Adicionalmente, de forma a não colocar a responsabilidade apenas numa pessoa, em caso de erro, toda a equipa é responsabilizada.

AC	Testes			Conclusão	
ID AC	**ID Teste**	**Descrição do teste a realizar**	**# ID Pedido**	**Teste**	**Conclusão do teste**
Gestão de Operações					
OP.01	Top.01	Verificar que está formalmente definido um procedimento de gestão de operações.	OPER.01	**Procedimento de teste ao D&I:** Não se encontra definido/ formalizado um procedimento de gestão de operações (gestão de *jobs*), que inclua os processos *job* existentes (nomeadamente os de maior criticidade), as normas e orientações relacionadas com a aprovação/ calendarização de jobs, assim como os procedimentos e responsáveis pela sua monitorização e correção. **OM** Apesar de não formalizado o procedimento formal para os sistemas em âmbito, de seguida é descrito como a gestão de operações é realizada na operadora, para os sistemas em âmbito: <u>Sistema Cobranças e Contabilidade</u> O processamento dos jobs de ambos os sistemas (Cobranças e Contabilidade), são realizados a partir de alertas (via email). A monitorização dos *jobs* é realizada pela DSI. Sempre que ocorre um erro que a DSI não tem *know-how* suficiente, recorre a um fornecedor externo. Adicionalmente, o processamento dos *jobs* é registado em *logs,* sempre que ocorre um erro a DSI analisa o log para auxiliar a resolução do mesmo. No entanto, a DSI não realiza qualquer relatório mensal da correção dos erros do processamento dos jobs. <u>Sistema Billing GSM</u> Os jobs do sistema *billing GSM* são geridos e monitorizados pelo parceiro de negócio do cliente, não sendo reportado qualquer relatório à operadora de monitorização dos jobs do sistema billing GSM, bem correção de erros.	**Efetivo**
OP.02	Top.02	Verificar se o acesso à calendarização de Jobs é restrito aos colaboradores autorizados.	OPER.11 OPER.22 OPER.32	**Procedimento de teste ao OE:** Através da análise à informação recebida, verificou-se que os acessos às aos *jobs* operacionais da operadora não são devidamente controlados, existindo um elevado número de administradores e de utilizadores com acessos desadequados face às suas necessidades. De seguida encontram-se listados a quantidade de administradores de com permissão para criação, alteração ou remoção de *jobs* operacionais, em cada sistema: - Sistema billing GSM: existem 15 utilizadores, dos quais 8 não necessitam do acesso para desempenhar as suas funções; - Sistema Cobranças: existem 10 utilizadores, dos quais 5 não necessitam do acesso para desempenhar as suas funções; e - Sistema Contabilidade: existem 23 utilizadores, dos quais 20 não necessitam do acesso para desempenhar as suas funções.	**Inefetivo**
OP.03	Top.03	Verificar se todas as	OPER.20	**Procedimento de teste ao OE:**	**Inefetivo**

		alterações realizadas aos Jobs são documentadas e aprovadas.	OPER.30 OPER.40 OPER.21 OPER.31 OPER.41	As alterações realizadas aos *jobs* aplicacionais definidos não são registadas/ documentadas, impossibilitando o *tracking* destas situações e o controlo/ monitorização das mesmas. Impossibilitando assim a resolução do presente teste.	
OP.04	Top.04	Verificar se estão definidos procedimentos formais para garantir que o processamento de Jobs (incluindo interfaces) é monitorizado e as exceções são devidamente acompanhadas e resolvidas (mecanismo de controlo de exceções).	OPER.01 OPER.12 OPER.13 OPER.14 OPER.15 OPER.23 OPER.24 OPER.25 OPER.26 OPER.33 OPER.34 OPER.35 OPER.36	**Procedimento de teste ao OE:** Verificámos que não se encontram formalmente definidos os procedimentos de monitorização e resolução de exceções no processamento dos *jobs* aplicacionais. <u>Sistema Cobranças</u> Apesar de não existir um procedimento formal para a monitorização e resolução de exceções no processamento de *jobs*, fomos informados que são gerados alertas diários no processamento dos mesmos. No entanto, a operadora apenas guarda logs dos últimos 2 meses. De forma a validar a operacionalidade deste controlo, selecionamos uma amostra (15 dias de 2015) de alertas e logs de execução dos *jobs*. No entanto, para (4/15) *jobs* que selecionamos para a amostra, não nos foi evidenciado qualquer informação. Adicionalmente, detetamos erros no processamento dos *jobs* para 2 dias de 2015 (8 Fev e 25-Mar). De modo a verificarmos a correção destes erros, solicitámos evidência da sua correção, no entanto, não nos foi evidenciado qualquer correção de erros. <u>Sistema Contabilidade</u> Apesar de não existir um procedimento formal para a monitorização e resolução de exceções no processamento de *jobs*, fomos informados que são gerados alertas diários no processamento dos mesmos. No entanto, a operadora apenas guarda logs dos últimos 2 meses. De forma a validar a operacionalidade deste controlo, selecionamos uma amostra (15 dias de 2015) de alertas e *logs* de execução dos *jobs*. Adicionalmente, detetamos erros no processamento dos jobs para 4 dias de 2015 (2-Fev 15-Fev 09-Mar e 27-Mar). De modo a verificarmos a correção destes erros, solicitámos evidência da sua correção. Para os dias 09 e 27 de Março, os problemas foram devidamente solucionados, os restantes erros não foi apresentado qualquer evidência de resolução. <u>Sistema Billing GSM</u> Fomos informados que o parceiro de negócio não reporta qualquer relatório de manutenção à operadora, bem como não armazena qualquer *log* de execução dos jobs do sistema. **OM**	**Inefetivo**

OP.05	Top.05	Verificar se estão definidos procedimentos para a realização de *backups*, incluindo procedimentos de monitorização dos *backups* para deteção e resolução de erros.	OPER.02	**Procedimento de teste ao D&I:** Não está formalmente definido/ documentado o procedimento de gestão de *backups,* que inclua, entre outros, a estratégia de *backups,* período de retenção, monitorização de *backups,* rotação de tapes para localização *off-site*. **OM** Apesar de não formalizado o procedimento formal para os sistemas em âmbito, de seguida é descrito como a gestão de *backups* é realizada na operadora, para os sistemas em âmbito: <u>Sistemas Cobranças e Contabilidade</u> Existe uma rotina de *backup* para o sistema Cobranças e duas rotinas de backup para o sistema Contabilidade, sendo todas as rotinas totais e diárias. Os *backups* são efetuados para tape, com um período de retenção é de 15 dias. Os jobs dos *backups* são monitorizados, diariamente através dos logs gerados pelos sistemas, por dois responsáveis da DSI. Quando ocorrem erros, estes analisam e tentam resolver o problema, se não tiverem o *know-how* suficiente, recorrem a um fornecedor externo. No entanto, a DSI não realiza qualquer relatório mensal da correção dos erros do processamento dos jobs de *backup*. <u>Sistema *billing GSM*</u> Fomos informados que os *jobs* dos *backups* são monitorizados pelo parceiro de negócio do cliente, não sendo reportado qualquer relatório à operadora de monitorização dos jobs de *backup* do sistema billing GSM, bem como correção de erros.	**Efetivo**
OP.06	Top.06	Verificar se o processo de *backups* está alinhado com a classificação da informação de acordo com a criticidade da mesma par ao negócio.	OPER.05 OPER.06	**Procedimento de teste o D&I e OE:** A informação não está classificada de acordo com a sua criticidade para o negócio.	**Inefetivo**
OP.07	Top.07	Verificar se o acesso à calendarização de *jobs* de *backup* é restrito aos colaboradores autorizados.	OPER.08	**Procedimento de teste à OE:** O acesso à alteração/ eliminação de *jobs* de *backups* encontra-se restrita a elementos da equipa de administração de sistemas.	**Efetivo**
OP.08	Top.08	Verificar se as alterações aos jobs de *backups* são devidamente documentadas e aprovadas.	OPER.09 OPER.10	**Procedimento de teste à OE:** As alterações realizadas aos *jobs* de *backups* definidos não são registadas, impossibilitando o *tracking* destas situações e o controlo/ monitorização das mesmas.	**Inefetivo**
OP.09	Top.09	Verificar se o processamento de jobs de *backup* é monitorizado e que as exceções são devidamente acompanhadas e	OPER.16 OPER.17 OPER.18 OPER.27 OPER.28	**Procedimento de teste à OE:** De forma a testar a operacionalidade deste controlo, solicitámos evidência da monitorização realizada ao processamento dos *backups,* bem como os *logs* de *backup* para os sistemas em âmbito. <u>Sistema Cobranças e Contabilidade</u> Os *jobs* de *backups* são monitorizados de forma *adhoc,* não existindo qualquer documentação	**Inefetivo**

		resolvidas.	OPER.29 OPER.37 OPER.38 OPER.39	decorrente da sua monitorização e correção de exceções. Contudo, fomos informados que a equipa da DSI monitoriza por observação, os seguintes alertas: - Alerta de espaço nas *tapes* dos servidores; - Alerta dos j*obs* de *backup* que falharam na sua execução; e - Alerta de bloqueio nos Servidores. <u>Sistema Billing GSM</u> Fomos informados que o parceiro de negócio não reporta qualquer relatório de manutenção ao cliente, bem como não armazena qualquer *log* de processamento dos *jobs* dos *backups*.	
OP.10	Top.10	Verificar se os *backups* são arquivados em localizações alternativas (off-site) para minimizar o risco de perda de dados.	OPER.03 OPER.04	**Procedimento de teste ao D&I e OE:** Não está formalmente definido um processo de envio das *tapes* de *backups* para *off-site*. Adicionalmente verificámos que não está a ser devidamente efetuado o armazenamento *off-site* das tapes de *backup*.	**Inefetivo**
OP.11	Top.11	Verificar se são realizados periodicamente testes de *restores* às tapes de *backups*.	OPER.07	**Procedimento de teste à OE:** Não existem evidências de testes de *restore* a *backups* realizados em 2014.	**Inefetivo**
Segurança da Informação					
SG.01	Tsg.01	Verificar se está formalmente definida uma política de segurança de informação.	SEG.01	**Procedimento de testes ao D&I:** Está definida e aprovada uma política de segurança da informação.	**Efetivo**
SG.02	Tsg.02	Verificar se está formalmente definida uma política de atribuição de nomes de utilizadores únicos para gestão dos acessos na Empresa.	SEG.08	**Procedimento de teste ao D&I:** Não existem procedimentos formalizados que definam uma nomenclatura de utilizadores e que reflita a prática utilizada informalmente na operadora.	**Inefetivo**

SG.03	Tsg.03	Verificar se estão formalmente definidos procedimentos de gestão de acessos aos sistemas da operadora.	SEG.02	**Procedimento de teste ao D&I:** Não está documentado o procedimento de gestão de acessos (i.e. criação, alteração, suspensão e revisão) aos sistemas da operadora. No entanto, quando é admitido um novo colaborador, o responsável de RH (com conhecimento do responsável da área) envia um email para o diretor da DSI a solicitar o acesso à rede e aos sistemas, com a definição do tipo de acesso pretendido. Quando é necessário efetuar uma alteração ao perfil de um utilizador, o responsável da área do colaborador envia um email ao diretor da DSI a solicitar a alteração do acesso e definição do novo perfil. Relativamente à remoção de utilizadores nos sistemas, sempre que um colaborador deixa de trabalhar na operadora, os recursos humanos (RH) enviam um email ao diretor da DSI, com essa informação. Após receção desse email, o coordenador DSI procede à desativação do utilizador na rede e sistemas.	**Inefetivo**
	Tsg.04	Verificar se estão formalmente definidos procedimentos de gestão de acessos de acesso à rede da operadora.	SEG.05	**Procedimento de teste ao D&I:** Não está documentado o procedimento de gestão de acessos (i.e. criação, alteração, suspensão e revisão) à rede da operadora. No entanto, quando é admitido um novo colaborador, o responsável de RH (com conhecimento do responsável da área) envia um email para o diretor da DSI a solicitar o acesso à rede e aos sistemas, com a definição do tipo de acesso pretendido. Quando é necessário efetuar uma alteração ao perfil de um utilizador, o responsável da área do colaborador envia um email ao diretor da DSI a solicitar a alteração do acesso e definição do novo perfil. Relativamente à remoção de utilizadores nos sistemas, sempre que um colaborador deixa de trabalhar na operadora, os recursos humanos (RH) enviam um email ao diretor da DSI, com essa informação. Após receção desse email, o coordenador DSI procede à desativação do utilizador na rede e sistemas.	**Inefetivo**
	Tsg.05	Verificar se estão formalmente definidos procedimentos para a atribuição, alteração e suspensão de acessos remotos.	SEG.04	**Procedimento de teste ao D&I:** Não está documentado o procedimento de gestão de acessos remotos (i.e. criação, alteração, suspensão e revisão).	**Inefetivo**

	Tsg.06	Verificar se estão formalmente definidos procedimentos para a atribuição, alteração e suspensão de acessos ao CPD.	SEG.03	**Procedimento de teste ao D&I:** Não está documentado o procedimento de gestão de acessos físicos (i.e. criação, alteração, suspensão e revisão) ao CPD da operadora.	**Inefetivo**
SG.04	Tsg.07	Validar se são comunicadas as saídas ou alterações de funções de colaboradores/ consultores externos à DSI e os acessos ajustados em conformidade.	GER.06 SEG.10	**Procedimento de teste OE:** Não existe/ não é mantida uma listagem com os colaboradores que saem da operadora, pelo que não é possível verificar se os acessos são suspensos e/ou readequados às alterações de funções.	**Inefetivo**
	Tsg.08	Verificar que não existem utilizadores com acessos à rede, acessos remotos, aos sistemas, às bases de dados e aos Data Centers, pertencentes a colaboradores/ consultores externos que já não exercem as respetivas funções na Empresa.	GER.06 SEG.18 SEG.22 SEG.23 SEG.31 SEG.28 SEG.39 SEG.33	**Procedimento de teste OE:** Para efetuar o teste à atividade de controlo em causa, solicitámos a listagem dos atuais colaboradores da Empresa. No entanto não nos foi disponibilizada a listagem dos colaboradores, o que impossibilita o teste (identificação de utilizadores ativos em sistema mas que já não fazem parte dos quadros da empresa).	**Inefetivo**
SG.05	Tsg.09	Verificar se os acessos à rede, às aplicações, sistemas operativos e bases de dados são revistos periodicamente pelos owners dos dados.	SEG.20 SEG.24 SEG.29 SEG.34	**Procedimento de teste à OE:** De forma a validar a operacionalidade deste controlo, solicitámos evidências das revisões efetuadas às aplicações, sistemas operativos e bases de dados No entanto, não existem relatórios de revisão aos acessos à rede, às aplicações, sistemas operativos e bases de dados, assinados e revistos periodicamente pelos *owners* dos dados.	**Inefetivo**
SG.06	Tsg.10	Validar se existe uma matriz de segregação de funções e se os conflitos de segregação de funções identificados são prontamente corrigidos.	SEG.09	**Procedimento de teste ao D&I e OE:** Não se encontra definida uma matriz de segregação de funções da Empresa que sirva de base à definição dos perfis de acesso implementados dos sistemas em âmbito, não sendo validado a possibilidade de atribuição de acessos com eventuais conflitos críticos.	**Inefetivo**
SG.07	Tsg.11	Verificar que a atribuição/ alteração de acessos ao sistema de Billing GSM é validada e devidamente aprovada.	SEG.23 SEG.25	**Procedimento de teste à OE:** De forma a verificarmos a operacionalidade deste controlo, solicitámos a listagem de utilizadores criados em 2014, para o sistema Billing GSM. Através da informação disponibilizada, verificámos que foram criados 10 novos utilizadores no	**Inefetivo**

			sistema Billing GSM. Da listagem, foram selecionados aleatoriamente, dois utilizadores e foi solicitado evidência do processo de pedido/ atribuição de acessos. No entanto, fomos informados que o parceiro de negócio, atribui acessos ao sistema Billing GSM de forma informal (telefone), sem que seja registado qualquer do processo de pedido/ atribuição de acessos.	
Tsg.12	Verificar que a atribuição/ alteração de acessos ao sistema de Cobranças é validada e devidamente aprovada.	SEG.28 SEG.33	**Procedimento de teste à OE:** De forma a verificarmos a operacionalidade deste controlo, solicitámos a listagem de utilizadores criados em 2014, para o sistema Cobrança. Através da informação disponibilizada, verificámos que foram criados 30 novos utilizadores no sistema Cobranças. Da listagem, foram selecionados aleatoriamente, cinco utilizadores e foi solicitado evidências do processo de pedido/ atribuição de acessos. Verificámos que 3/5 foram devidamente aprovados pelo responsável dos RH e que os acessos foram devidamente criados pelo diretor da DSI. Para os restantes casos da amostra, 2/5, não foram disponibilizados quaisquer evidências do pedido e respectiva aprovação do acesso	**Inefetivo**
Tsg.13	Verificar que a atribuição/ alteração de acessos ao sistema de Contabilidade é validada e devidamente aprovada.	SEG.33 SEG.41	**Procedimento de teste à OE:** De forma a verificarmos a operacionalidade deste controlo, solicitámos a listagem de utilizadores criados em 2014, para o sistema Contabilidade. Através da informação disponibilizada, verificámos que foram criados 35 novos utilizadores no sistema Contabilidade. Da listagem, foram selecionados aleatoriamente, cindo utilizadores e foi solicitado evidências do processo de pedido/ atribuição de acessos. Verificámos que 3/5 foram devidamente aprovados pelo responsável dos RH e que os acessos foram devidamente criados pelo diretor da DSI. No entanto, para 1/5 não existiu, aprovação por parte do responsável de RH, mas sim pelo diretor Financeiro, tendo sido também criado pelo diretor da DSI. Para o restante caso da amostra, 1/5, não foi disponibilizado quaisquer evidência do pedido e respectiva aprovação do acesso.	**Inefetivo**
Tsg.14	Verificar que a atribuição/ alteração de acessos à *Active Directory* é validada e devidamente aprovada.	SEG.18 SEG.18	**Procedimento de teste à OE:** De forma a verificarmos a operacionalidade deste controlo, solicitámos a listagem de utilizadores criados em 2014, na *Active Directory*. Através da informação disponibilizada, verificámos que foram criados 60 novos utilizadores no sistema Contabilidade. Da listagem, foram selecionados aleatoriamente, 15 utilizadores e foi	**Inefetivo**

				solicitado evidências do processo de pedido/ atribuição de acessos. Verificámos que 6/15 foram devidamente aprovados pelo responsável dos RH e que os acessos foram devidamente criados pelo diretor da DSI; 4/ 15 são consultores externos que não existe qualquer aprovação por parte dos RH, existe apenas um email do diretor da DSI para um dos consultores externos a notificar que o acesso foi criado; e para os restantes casos da amostra, 5/15, não foi disponibilizado quaisquer evidências do pedido e respectiva aprovação do acesso.	
SG.08	Tsg.15	Verificar se os privilégios de acesso "super user" / administrador nas aplicações e bases de dados apenas são atribuídos quando realmente necessário e todas as ações são registadas e revistas pela gestão.	SEG.23 SEG.28 SEG.33 SEG.18 SEG.22 SEG.31 SEG.32	**Procedimento de teste à OE:** De forma a testarmos a operacionalidade deste controlo, foram solicitadas as listagens de utilizadores e respetivos perfis de acesso às aplicações, bases de dados e sistema operativo dos sistemas em âmbito (Billing GSM, Cobranças e Contabilidade) e AD. <u>Sistema Billing GSM:</u> - Aplicação: existem 12 utilizadores genéricos com acesso alargado ao sistema Billing GSM; - BD: existem 5 utilizadores genéricos com acesso de alargado à BD do sistema Billing GSM (acesso direto). - SO: existem 2 utilizadores genéricos com acesso de administração do SO do sistema Billing GSM. <u>Sistema Cobranças:</u> - Aplicação: existem 10 utilizadores genéricos com acesso alargado ao sistema Cobranças. - BD: existem 9 utilizadores genéricos com acesso de alargado à BD do sistema Cobranças (acesso direto). - SO: existem 8 utilizadores genéricos com acesso de administração do SO do sistema Cobranças. <u>Sistema Contabilidade:</u> - Aplicação: existem 12 utilizadores genéricos com acesso alargado ao sistema Contabilidade - BD: não nos foi fornecido qualquer listagem dos utilizadores com acesso à BD do sistema Contabilidade - SO: existem 8 utilizadores genéricos com acesso de administração do SO do sistema Contabilidade <u>AD</u> - Existem 21 utilizadores com perfil de Administração (*domain admin*).	**Inefetivo**

SG.09	Tsg.16	Verificar se estão implementados controlos de forma a identificar univocamente o utilizador responsável pelas operações realizadas nas aplicações e bases de dados (user ids únicos e não partilhados).	SEG.39 SEG.23 SEG.31 SEG.28 SEG.32 SEG.33	**Procedimento de teste à OE:** De forma a testarmos a operacionalidade deste controlo, foram solicitadas as listagens de utilizadores e respetivos perfis de acesso às aplicações, bases de dados e sistema operativo dos sistemas em âmbito (Billing GSM, Cobranças e Contabilidade) e AD. Através da análise da listagem de utilizadores dos sistemas em âmbito (billing GSM, Cobranças e Contabilidade) e AD, verificámos que: <u>Sistema Billing GSM</u>: - Aplicação: existem 40 utilizadores genéricos. - BD: existem 8 utilizadores genéricos. - SO: existem 5 utilizadores genéricos. <u>Sistema Cobranças:</u> - Aplicação: existem 28 utilizadores genéricos. - BD: existem 12 utilizadores genéricos. - SO: existem 6 utilizadores genéricos. <u>Sistema Contabilidade:</u> - Aplicação: existem 27 utilizadores genéricos. - BD: não nos foi fornecido qualquer listagem dos utilizadores com acesso à BD. - SO: existem 6 utilizadores genéricos. <u>AD:</u> - Existem 50 utilizadores genéricos; e - Existem 6 utilizadores duplicados (o mesmo colaborador está associado a dois *users* distintos).	**Inefetivo**
SG.10	Tsg.17	Verificar se estão definidos parâmetros de autenticação (e.g., *Password Minimum Length* & *Complexity*, *Password Expiration, Account Lockout*, etc.) para acesso às aplicações e bases de dados.	SEG.19 SEG.25 SEG.30	**Procedimento de teste à OE:** De forma a testar a operacionalidade deste controlo, solicitámos os parâmetros de segurança dos sistemas em âmbito (Billing GSM, Cobranças e Contabilidade) e AD. Através da informação recebida verificámos que: Active *Directory*: Da análise efetuada verificámos que: - *Minimum Password Length* - (Tamanho mínimo para definição de password) - Está configurado com 4 carateres e o descrito na política de segurança de informação é que sejam 6 ou mais caracteres; - *Maximum password age* - (Número máximo de dias que a password é válida) - Está configurado *Not defined*, e o recomendado é que esteja entre 30 e 90; - *Minimum password age* - (Número mínimo de dias que a password é válida) - Está configurada Not	**Inefetivo**

			SEG.35	*defined*, e o recomendado que esteja entre 0 e 1 dias; - *Password must meet complexity requirements* - (Nível de complexidade da password) - Está configurada *Not defined*, e o recomendado que este parâmetro esteja *Enabled*; e - *Reversible password encryption* (Impossibilidade de utilização de algoritmos de cifra reversíveis) - Está configurada *Not defined*, e o recomendado que este parâmetro esteja *Disabled*. Relativamente aos restantes sistemas, em reunião foi-nos comunicado não seria possível extrair esta informação.	
SG.11	Tsg.18	Verificar se existe *software* antivírus instalado nos computadores ligados à rede para garantir a segurança dos sistemas, programas e dados evitando alterações não autorizadas. A lista de vírus conhecidos é atualizada adequadamente e regularmente. Todos os programas e ficheiros existentes na rede são verificados regularmente.	SEG.16 SEG.17	**Procedimento de teste ao D&I e OE:** Verificámos que existe um *software* antivírus instalado e estão definidas configurações padronizadas pelos computadores ligados à rede. São realizados periodicamente, nos diversos computadores, scans e refletidas as atualizações.	**Efetivo**
SG.12	Tsg.19	Verificar se existe um controlo e uma segregação da rede, de forma a proteger os sistemas mais críticos de acessos não autorizados.	GER.02	**Procedimento de testes ao D&I e OE:** Não existe um desenho atualizado da rede da operadora.	**Inefetivo**
	Tsg.20	Verificar se existem ferramentas ou funcionalidades que permitam o registo de tentativas de acesso, acessos com e sem sucesso. Adicionalmente, verificar se estes eventos são devidamente	SEG.15	**Procedimento de teste de D&I e OE:** Relativamente às ferramentas de monitorização de acessos e eventos de segurança o único sistema que efetua este registo é a AD *(Audit Policy)* sendo que os restantes sistemas não monitorizam este tipo de eventos. Não se encontra definido o processo de monitorização, e tomada de ações caso necessário, deste tipo de eventos.	**Inefetivo**

		monitorizados e acompanhadas as exceções.			
SG.13	Tsg.21	Verificar se estão documentados os procedimentos de controlo de acessos físicos que permitam restringir e registar os acessos o CPD.	SEG.03	**Procedimento de teste ao D&I:** Verificámos que não se encontra definida/ formalizada uma política empresarial de segurança da informação alinhada com as boas práticas de mercado, na qual deveriam ser considerados os sistemas de informação, as instalações e a proteção dos recursos humanos. No entanto, o procedimento realizado pela operadora é o seguinte: O acesso ao edifício é controlado através de seguranças que se encontram na receção, sendo o acesso efetuado através de cartão de identificação (com fotografia). O acesso ao centro de processamento de dados (CPD) é realizado através de cartão magnético, onde se encontram localizados os servidores dos sistemas de Cobranças e Contabilidade, efetuado com cartão magnético, existindo um registo em logs desses acessos. Relativamente ao acesso físico ao CPD por parte de visitantes/ fornecedores externos, é efetuado através do acompanhamento de um dos colaboradores com acesso. A responsabilidade da atribuição e recolha dos cartões magnéticos que permitem o acesso físico ao CPD é da responsabilidade da administração da operadora. No entanto, não estão formalmente definidos procedimentos de gestão e controlo dos acessos físicos.	**Efetivo**
	Tsg.22	Verificar se os acessos ao CPD são devidamente controlados e registados.	SEG.07 N/A SEG.06	**Procedimento de teste à OE:** De forma a testarmos a operacionalidade deste controlo, foram solicitados os *logs* de acesso ao CPD. Através da análise à informação recebida verificámos os acessos ao CPD são devidamente registados em *logs*. No entanto, os *logs* encontram-se generalizados, o que impossibilita a distinção dos colaboradores.	**Inefetivo**
	Tsg.23	Verificar se os registos dos acessos físicos ao CPD, edifício sede e armazéns são revistos periodicamente.	SEG.11	**Procedimento de teste à OE:** Não são revistos periodicamente os registos dos acessos físicos ao CPD e edifício sede.	**Inefetivo**

SG.14	Tsg.24	Verificar se estão documentados procedimentos formais de gestão dos acessos físicos (i.e. criação, alteração, suspensão e revisão de acessos) e estão definidas e atribuídas responsabilidades, de forma a que apenas um número limitado de pessoas pode efetuar alterações às autorizações.	SEG.02	**Procedimento de teste ao D&I:** Não estão documentados os procedimentos de gestão dos acessos físicos (i.e. criação, alteração, suspensão e revisão de acessos) e estão definidas e atribuídas responsabilidades, de forma a que apenas um número limitado de pessoas pode efetuar alterações às autorizações. Adicionalmente, fomos informados que a responsabilidade da atribuição e recolha dos cartões magnéticos que permitem o acesso físico ao CPD é da responsabilidade da administração da operadora.	**Inefetivo**
	Tsg.25	Verificar se os acessos físicos aos data centers estão devidamente aprovados.	SEG.06 SEG.12	**Procedimento de teste à OE:** De forma a testarmos a operacionalidade deste controlo, solicitámos a lista de pessoas autorizadas a aceder ao CPD. Da listagem, foi selecionada uma amostra de 5 colaboradores para os quais solicitámos aprovação formal. No entanto, fomos informados que não existem evidências de aprovação dos acessos físicos dos colaboradores ao CPD.	**Inefetivo**
SG.15	Tsg.26	Verificar se a saída/alteração de funções de colaboradores é comunicada para que possam ser eliminados/ajustados os acessos físicos à informação.	GER.07 SEG.13	**Procedimento de teste à OE:** De forma a testarmos a operacionalidade deste controlo, solicitámos a listagem dos colaboradores que saíram dos quadros da operadora durante o ano de 2014. No entanto, fomos informados que não existe uma listagem com as movimentações de colaboradores da operadora (saídas e/ou alterações de funções). Deste modo não é possível verificar se as saídas/alterações de funções são comunicadas e os acessos readequados à situação.	**Inefetivo**
SG.16	Tsg.27	Verificar se está definido um plano de continuidade de negócio e um plano de recuperação de desastres.	SEG.14	**Procedimento de teste ao D&I e OE:** Não se encontra definido e implementado um plano de *disaster recovery plan* (DRP) e *business coninuity planing* (BCP), assim como não é realizado o armazenamento *off-site* das tapes de *backups*.	**Inefetivo**

SG.17	Tsg.28	Verificar se está definido um plano de que contemple a segurança física do CPD, existem fontes de alimentação alternativas (e.g. fornecimento de energia ininterrupto, geradores, etc) e controlos de proteção do ambiente de processamento.	N/A	**Procedimento de teste ao D&I e OE:** O centro de processamento de dados (CPD) está localizado nas instalações edifício sede da Empresa, em Luanda, nas instalações da DSI. Embora não estejam documentadas as regras/ políticas de segurança ambiental que devem estar implementadas, através de uma visita realizada ao CPD, verificámos as seguintes vulnerabilidades, nomeadamente: - Não existe um diagrama com identificação de áreas classificadas como criticas e políticas, procedimentos, normas e orientações relacionadas com a administração da segurança física; - Não possui monitorização local de temperatura e não existe um sistema de monitorização da humidade com alerta para níveis de humidade fora dos parâmetros definidos; - A porta do CPD não é blindada e as paredes não são resistentes ao fogo; - Não existem mecanismos automáticos de extinção de incêndios; - Não existe nenhum extintor manual no interior do CPD; - Existem materiais inflamáveis no interior do CPD, designadamente papel e cartão; - Não existe manutenção periódica dos equipamentos de ar condicionado; - O CPD está desprovido de um sistema de monitorização por meio de circuito interno de vídeo; - Os *racks* com equipamento ativo (servidores, *switches*, routers, equipamento de comunicações) não se encontram devidamente trancados; - Não existe nenhum registo formalizado com os acessos efetuados ao CPD; - Não existe uma porta de saída de emergência, as portas do CPD devem abrir para o exterior e devem ter barras de saída rápida; e - As UPS não têm manutenções periódicas nem são testadas regularmente quanto ao seu correto funcionamento.	**Inefetivo**
Gestão de Alterações					

ALT.01	Tal.01	Verificar se é utilizada uma metodologia ou processo, devidamente aprovado, relativo à modificação dos sistemas aplicacionais de forma a garantir consistência no desenvolvimento da alteração.	ALT.01	**Procedimento de teste ao D&I:** Verificámos que está formalmente descrito o procedimento de gestão de alterações que descreva as seguintes principais fases e responsabilidades: (i) Definição de requisitos; (ii) Análise e aprovação; (iii) Desenvolvimento; (iv) Testes (e.g. de carga, técnicos, de aceitação); e (v) Aprovação da passagem a produção. O procedimento documentado instituiu a seguinte metodologia: o pedido de desenvolvimento é realizado junto da DSI é efetuado com recurso ao email já após a aprovação do responsável de negócio (por vezes informalmente). Após o pedido é efetuada uma análise de requisitos e viabilidade incluindo o tempo e custo para o desenvolvimento. Caso o projeto seja aceite, avança-se para o desenvolvimento e testes. Os testes são aprovados pelos *key-users* antes da passagem a produção. Adicionalmente, as alterações ao sistema Billing GSM, são da total responsabilidade do parceiro de negócio. No entanto, todas as alterações realizadas ao sistema Billing GSM têm de ser notificadas e aprovadas pelo PMO (*Project Management Office*) da operadora. <u>Sistema Operativo</u> Verificámos que não se encontram formalizados e documentados os procedimentos de instalação e realização de testes, antes da instalação em produção de *updates*/ *patches* do sistema operativo. Apesar de não existir um procedimento definido/ documentado, quando existem novos *patches*/ atualizações comunicados pelo fornecedor (Microsoft), a DSI faz as atualizações de acordo com as especificações fornecidas pelo fornecedor. <u>Bases de dados</u> As alterações às bases de dados são, por norma, realizadas no âmbito de alterações aplicacionais, sendo geridas no âmbito destas e de acordo com o procedimento de gestão de alterações definido/ implementado.	**Efetivo**
ALT.02	Tal.02	Verificar se as alterações às aplicações, bases de dados e sistema operativo são aprovadas.	ALT.03 ALT.08 ALT.13 ALT.02 ALT.07 ALT.12 ALT.05 ALT.10 ALT.15 ALT.17 ALT.04	**Procedimento de teste à OE:** De forma a testarmos esta atividade de controlo, obtivemos a listagem de alterações (manutenção evolutiva e corretiva) introduzidas nos sistemas em âmbito (Billing GSM, Cobranças e Contabilidade) durante o ano de 2014 e solicitámos a documentação da alteração. <u>Sistema Billing GSM</u> Aplicacional A partir da listagem de alterações do sistema Billing GSM, selecionámos 5 alterações como amostra e solicitamos a aprovação do pedido de alteração.	**Inefetivo**

ALT.09 ALT.14 ALT.06 ALT.11 ALT.16	Através da informação disponibilizada, verificámos que apenas 2/5 alterações estão acompanhadas pela aprovação da alteração. O processo de aprovação não é realizado de forma uniforme/ consistente (as aprovações estão dispersas por vários emails trocados) entre o parceiro de negócio e o PMO da operadora. Adicionalmente, não existe aprovação formal dentro do parceiro de negócio. Sistema Operativo A partir da listagem de alterações realizadas ao sistema operativo, foram selecionadas, 5 alterações como amostra e solicitámos a aprovação do pedido de alteração. No entanto, o parceiro de negócio instala os novos patches/ atualizações comunicados pelo fornecedor (Microsoft), sem que dada qualquer aprovação prévia. Base de dados Quanto às atualizações à base de dados que suportam o sistema Billing GSM, fomos informados que não existiram alterações durante 2014, pelo que não existem eventos a testar. <u>Sistema Cobranças</u> Aplicacional A partir da listagem de alterações do sistema Cobranças, selecionámos 10 alterações como amostra e solicitamos a aprovação do pedido de alteração. Através da informação disponibilizada, verificámos que apenas 7/10 alterações estão acompanhadas pela aprovação da alteração. Os responsáveis do negócio (e.g. diretor dos RH) notificam a DSI da necessidade de alteração ao sistema. Para as restante alterações (3/10) não existe qualquer evidência de aprovação. Sistema Operativo A partir da listagem de alterações realizadas ao sistema operativo, foram selecionadas, 5 alterações como amostra e solicitámos a aprovação do pedido de alteração. No entanto, o parceiro de negócio instala os novos patches/ atualizações comunicados pelo fornecedor (Microsoft), sem que dada qualquer aprovação prévia. Base de dados Quanto às atualizações à base de dados que suportam o sistema Cobranças, fomos informados que não existiram alterações durante 2014, pelo que não existem eventos a testar. <u>Sistema Contabilidade</u> Aplicacional A partir da listagem de alterações do sistema Cobranças, selecionámos 5 alterações como amostra e solicitamos a aprovação do pedido de alteração.	

				Através da informação disponibilizada, verificámos que apenas 4/5 alterações estão acompanhadas pela aprovação da alteração. Os responsáveis do negócio (e.g. diretor dos RH) notificam a DSI da necessidade de alteração ao sistema. Para a restante alteração (1/5) não existe qualquer evidência de aprovação. Sistema Operativo A partir da listagem de alterações realizadas ao sistema operativo, foram selecionadas, 5 alterações como amostra e solicitámos a aprovação do pedido de alteração. No entanto, o parceiro de negócio instala os novos patches/ atualizações comunicados pelo fornecedor (Microsoft), sem que dada qualquer aprovação prévia. Base de dados Quanto às atualizações à base de dados que suportam o sistema Contabilidade, fomos informados que não existiram alterações durante 2014, pelo que não existem eventos a testar.	
ALT.03	Tal.03	Verificar se alterações às aplicações, bases de dados e sistema operativo são devidamente testadas de forma a garantir que estão em conformidade com os requisitos definidos.	ALT.03 ALT.08 ALT.13 ALT.02 ALT.07 ALT.12 ALT.05 ALT.10 ALT.15 ALT.17 ALT.04 ALT.09 ALT.14 ALT.06 ALT.11 ALT.16	**Procedimento de teste à OE:** De forma a testarmos esta atividade de controlo, obtivemos a listagem de alterações (manutenção evolutiva e corretiva) introduzidas nos sistemas em âmbito (Billing GSM, Cobranças e Contabilidade) durante o ano de 2014 e solicitámos a documentação da alteração. **Sistema Billing GSM** Aplicacional A partir da listagem de alterações do sistema Billing GSM, selecionámos 5 alterações como amostra e solicitamos os testes realizados antes da passagem a produção. Através da informação disponibilizada, verificámos que apenas 3/5 alterações foram realizados teste pelos *key-users* antena da passagem a produção. As restantes 2/5 alterações não foram efetuados quaisquer testes antes da passagem a produção. Sistema Operativo A partir da listagem de alterações realizadas ao sistema operativo, foram selecionadas, 5 alterações como amostra e solicitámos a aprovação do pedido de alteração. No entanto, o parceiro de negócio instala os novos patches/ atualizações comunicados pelo fornecedor (Microsoft), sem que seja realizado qualquer teste. Base de dados Quanto às atualizações à base de dados que suportam o sistema Billing GSM, fomos informados que não existiram alterações durante 2014, pelo que não existem eventos a testar. Sistema Cobranças	**Inefetivo**

				Aplicacional A partir da listagem de alterações do sistema Cobranças, selecionámos 10 alterações como amostra e solicitamos os testes realizados antes da passagem a produção. Através da informação disponibilizada, verificámos que apenas 5/10 alterações realizadas ao sistema Cobranças, foram realizados testes pelos key-users, antes da passagem a produção. Para as restantes alterações (5/10) não existe evidência de testes realizados. Sistema Operativo A partir da listagem de alterações realizadas ao sistema operativo, foram selecionadas, 5 alterações como amostra e solicitámos a aprovação do pedido de alteração. No entanto, o parceiro de negócio instala os novos patches/ atualizações comunicados pelo fornecedor (Microsoft), sem que seja realizado qualquer teste. Base de dados Quanto às atualizações à base de dados que suportam o sistema Cobranças, fomos informados que não existiram alterações durante 2014, pelo que não existem eventos a testar. **Sistema Contabilidade** Aplicacional A partir da listagem de alterações do sistema Cobranças, selecionámos 5 alterações como amostra e solicitamos os testes realizados antes da passagem a produção. Através da informação disponibilizada, verificámos que apenas 2/5 alterações foram realizados testes pelos *key-users*, antes da passagem a produção. Os responsáveis do negócio (e.g. diretor dos RH) notificam a DSI da necessidade de alteração ao sistema. Para as restante alterações (3/5) não existe evidência de testes realizados. Sistema Operativo A partir da listagem de alterações realizadas ao sistema operativo, foram selecionadas, 5 alterações como amostra e solicitámos a aprovação do pedido de alteração. No entanto, o parceiro de negócio instala os novos patches/ atualizações comunicados pelo fornecedor (Microsoft), sem que seja realizado qualquer teste. Base de dados Quanto às atualizações à base de dados que suportam o sistema Contabilidade, fomos informados que não existiram alterações durante 2014, pelo que não existem eventos a testar.	
ALT.04	Tal.04	Verificar se os testes realizados às alterações de	ALT.03 ALT.08	**Procedimento de teste à OE:**	**Inefetivo**

aplicações e bases de dados são aprovados pelo negócio antes da passagem a produção	ALT.13 ALT.02 ALT.07 ALT.12 ALT.05 ALT.10 ALT.15 ALT.17 ALT.04 ALT.09 ALT.14 ALT.06 ALT.11 ALT.16	De forma a testarmos esta atividade de controlo, obtivemos a listagem de alterações (manutenção evolutiva e corretiva) introduzidas nos sistemas em âmbito (Billing GSM, Cobranças e Contabilidade) durante o ano de 2014 e solicitámos a documentação da alteração. <u>Sistema Billing GSM</u> Aplicacional A partir da listagem de alterações do sistema Billing GSM, selecionámos 5 alterações como amostra e solicitamos as aprovações antes da passagem a produção. Através da informação disponibilizada, verificámos que apenas 2/5 existe aprovação formal para colocar a alteração em produção. As restantes 2/5 alterações não existiu qualquer aprovação antes da entrada em produção. Sistema Operativo A partir da listagem de alterações realizadas ao sistema operativo, foram selecionadas, 5 alterações como amostra e solicitámos a aprovação do pedido de alteração. No entanto, o parceiro de negócio instala os novos patches/ atualizações comunicados pelo fornecedor (Microsoft), sem que dada qualquer aprovação antes da entrada em produção. Base de dados Quanto às atualizações à base de dados que suportam o sistema Billing GSM, fomos informados que não existiram alterações durante 2014, pelo que não existem eventos a testar. <u>Sistema Cobranças</u> Aplicacional A partir da listagem de alterações do sistema Cobranças, selecionámos 10 alterações como amostra e solicitamos as aprovações antes da passagem a produção. Através da informação disponibilizada, verificámos que apenas 4/10 existe aprovação formal para colocar a alteração em produção. As restantes 6/10 alterações não existiu qualquer aprovação antes da entrada em produção. Sistema Operativo A partir da listagem de alterações realizadas ao sistema operativo, foram selecionadas, 5 alterações como amostra e solicitámos a aprovação do pedido de alteração. No entanto, o parceiro de negócio instala os novos patches/ atualizações comunicados pelo fornecedor (Microsoft), sem que dada qualquer aprovação antes da entrada em produção. Base de dados	

				Quanto às atualizações à base de dados que suportam o sistema Cobranças, fomos informados que não existiram alterações durante 2014, pelo que não existem eventos a testar. <u>Sistema Contabilidade</u> Aplicacional A partir da listagem de alterações do sistema Cobranças, selecionámos 5 alterações como amostra e solicitamos as aprovações antes da passagem a produção. Através da informação disponibilizada, verificámos que apenas 2/5 existe aprovação formal para colocar a alteração em produção. As restantes 3/5 alterações não existiu qualquer aprovação antes da entrada em produção. Sistema Operativo A partir da listagem de alterações realizadas ao sistema operativo, foram selecionadas, 5 alterações como amostra e solicitámos a aprovação do pedido de alteração. No entanto, o parceiro de negócio instala os novos patches/ atualizações comunicados pelo fornecedor (Microsoft), sem que dada qualquer aprovação antes da entrada em produção. Base de dados Quanto às atualizações à base de dados que suportam o sistema Contabilidade, fomos informados que não existiram alterações durante 2014, pelo que não existem eventos a testar.	
Fornecedores externos					
FR.01	Forn.01	Verificar se o contro entre a operadora e o parceiro de negócio se encontra em vigor	GER.03	Através da informação recebida, verificámos que o contrato entre a operadora e o parceiro de negócio da operadora se encontra em vigor.	**Efetivo**

Testes – Integração

Testes		Conclusões		
#ID Teste a realizar	Descrição do teste a realizar	#ID Evidência	Teste	Conclusão do teste
Consumos				
Tin.01	Verificar que os dados dos consumos de saldo em números pré-pagos GSM, extraídos do sistema de *billing* GSM para integração na contabilidade, correspondem ao período de faturação correto e incluem todos os dias do período.	INT.05 INT.06	Para a realização do presente teste, solicitámos dois ficheiros contendo a informação dos consumos. Esta informação é disponibilizada mensalmente pelo parceiro de negócio à operadora. Através da análise à informação recebida, foi detetado que a operadora não considerava o dia um dia por mês na faturação (o período de faturação corresponde ao período entre o dia 25 do mês anterior e o dia 24 do mês corrente, inclusive).	**Inefetivo**
Tin.02	Verificar que os dados extraídos do *billing* GSM, para integração na contabilidade, representam os dados de consumo de saldo em números pré-pagos GSM que estão registados no *billing*.	INT.05 INT.06	Para a realização do presente teste, solicitámos dois ficheiros contendo a informação dos consumos. Esta informação é disponibilizada mensalmente pelo parceiro de negócio à operadora. Através da análise à informação, foram identificadas diferenças entre os dados disponibilizados pelo parceiro de negócio (entre o detalhe e o resumo dos consumos dos números pré-pagos GSM)	**Inefetivo**
Tin.03	Verificar que os dados de consumos de saldo em números pré-pagos GSM carregados na interface *Cobrança s& Consumos*, resultantes do processo de preparação da informação para integração na contabilidade, correspondem aos dados registados e extraídos do sistema de *billing* GSM.	INT.08 INT.09 INT.11 INT.05 INT.01	Através da análise à informação recebida, identificámos produtos que não estavam a ser considerados na contabilidade. Aquando do carregamento dos dados na interface Cobranças & Consumos a listagem dos produtos que se encontravam definidos na Contabilidade não continha todos os produtos, rejeitando assim, os produtos que se encontravam no sistema de Billing GSM.	**Inefetivo**
Tin.04	Verificar que os dados de consumos de saldo em números pré-pagos GSM refletidos nas rúbricas de contabilidade são validados antes da sua contabilização, estão íntegros e enquadram-se nas espectativas da área financeira.	INT.01	Não existe uma validação das rubricas contabilísticas antes da sua contabilização.	**Inefetivo**
Tin.05	Verificar que os dados de carregamentos de saldo em números pré-pagos GSM estão corretamente refletidos nas rúbricas de contabilidade (i.e. os valores são iguais aos que estão na interface *Cobranças&Consumos Log* e as rúbricas	INT.01 INT.02	Através da análise à informação recebida, foram detetadas diferenças entre os montantes que se encontravam na interface Cobranças & Consumos *Log* com o montante se se encontrava nas rubricas (General Ledger).	**Inefetivo**

	atualizadas foram as validadas).			
Carregamentos				
Tin.06	Verificar que os dados dos carregamentos de saldo em números pré-pagos GSM, extraídos do sistema de *billing* GSM para integração na contabilidade, correspondem ao período de faturação correto e incluem todos os dias do período.	INT.03 INT.04	Para a realização do presente teste, solicitámos dois ficheiros contendo a informação dos carregamentos Esta informação é disponibilizada mensalmente pelo parceiro de negócio à operadora. Através da análise à informação recebida, foi detetado que a operadora não considerava o dia um dia por mês na faturação (o período de faturação corresponde ao período entre o dia 25 do mês anterior e o dia 24 do mês corrente, inclusive).	**Inefetivo**
Tin.07	Verificar que os dados extraídos do *billing* GSM, para integração na contabilidade, representam os dados de carregamentos de saldo em números pré-pagos GSM que estão registados no *billing*.	INT.03 INT.04	Para a realização do presente teste, solicitámos dois ficheiros contendo a informação dos carregamentos. Esta informação é disponibilizada mensalmente pelo parceiro de negócio à operadora. Através da análise à informação, foram identificadas diferenças entre os dados extraídos do billing GSM e os dados registados no *billing*.	**Inefetivo**
Tin.08	Verificar que os dados de carregamentos de saldo em números pré-pagos GSM carregados na interface *Cobranças & Consumos*, resultantes do processo de preparação da informação para integração na contabilidade, correspondem aos dados registados e extraídos do sistema de *billing* GSM.	INT.10 INT.07 INT.09 INT.11 INT.03 INT.01	Através da análise à informação recebida, identificámos produtos que não estavam a ser considerados na contabilidade. Aquando a importação dos dados na interface Cobranças & Consumos a listagem dos produtos que se encontravam definidos na Contabilidade não continha todos os produtos, rejeitando assim, os produtos que se encontravam no sistema de *Billing* GSM.	**Inefetivo**
Tin.09	Verificar que os dados de carregamentos de saldo em números pré-pagos GSM refletidos nas rúbricas de contabilidade são validados antes da sua contabilização, estão íntegros e enquadram-se nas espectativas da área financeira	INT.10 INT.01	Através da análise à informação recebida, verificou-se que não existe qualquer controlo aos dados dos carregamentos de saldo dos números pré-pagos GSM refletidos nas rúbricas contabilísticas.	**Inefetivo**
Tin.10	Verificar que os dados de carregamentos de saldo em números pré-pagos GSM estão corretamente refletidos nas rúbricas de contabilidade (i.e. os valores são iguais aos que estão na interface *Cobranças & Consumos Log* e as rubricas atualizadas foram as validadas).	INT.10 INT.02 INT.01	Através da análise à informação recebida, foram detetadas diferenças entre os montantes que se encontravam na interface Cobranças & Consumos Log com o montante que se encontrava nas rubricas (General Ledger). Adicionalmente, verificou-se mais uma vez neste teste que os existem produtos que estavam a ser desconsiderados na contabilidade.	**Inefetivo**